OECD Reviews of Digital Transformation

Going Digital in Latvia

OECD

OECD Reviews of Digital Transformation

Going Digital in Latvia

OECD
BETTER POLICIES FOR BETTER LIVES

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

Please cite this publication as:
OECD (2021), *Going Digital in Latvia*, OECD Reviews of Digital Transformation, OECD Publishing, Paris, *https://doi.org/10.1787/8eec1828-en*.

ISBN 978-92-64-55190-9 (print)
ISBN 978-92-64-83854-3 (pdf)

OECD Reviews of Digital Transformation
ISSN 2708-9150 (print)
ISSN 2708-9169 (online)

Photo credits: Cover © Adobe Stock/Image design © Taï Marc Le Than.

Corrigenda to publications may be found on line at: *www.oecd.org/about/publishing/corrigenda.htm*.

© OECD 2021

The use of this work, whether digital or print, is governed by the Terms and Conditions to be found at *http://www.oecd.org/termsandconditions*.

Foreword

Going Digital in Latvia is part of a new series of OECD country reviews. The OECD Reviews of Digital Transformation examine recent country developments in the digital economy, analyse policies related to digitalisation and make recommendations to increase policy coherence in this area.

Going Digital in Latvia explores recent developments in infrastructure for the digital economy, telecom markets, and related regulations and policies in Latvia. It reviews trends in the use of digital technologies by individuals, businesses and the government, and examines policies to foster diffusion. The Review also analyses opportunities and challenges raised by digitalisation in key areas and evaluates policy responses to these changes. The areas covered range from innovation and skills to digital security and data governance.

The Review considers these policies in relation to their coherence among different domains in order to foster synergies across government ministries and institutions, based on the OECD Going Digital Integrated Policy Framework.

Going Digital in Latvia was undertaken following an invitation by the Ministry of Environmental Protection and Regional Development of the Republic of Latvia, which also provided financial support. The Review was carried out by the OECD Directorate for Science, Technology and Innovation under the auspices of the OECD Committee on Digital Economy Policy.

The Review was prepared by a team led by Vincenzo Spiezia and including Duncan Cass-Beggs, Ghislain De Salins, Rory O'Farrell, Joshua Polchar, Lorrayne Porciuncula, Elettra Ronchi, Julia Staudt, Jan Tscheke and Akira Yoshida, under the supervision of Anne Carblanc and Audrey Plonk, respectively the former and current Head of the Digital Economy Division. The Review has also benefited from comments by Hermann Garden, Oscar Huerta Melchor, Gernot Hutschenreiter, George Kamiya, Kenza Khachani, Soo-Jin Kim, Aline Matta, Jilian Oderkirk, Atsuhito Oshima and Dirk Pilat.

The authors owe much to the support and co-operation of the Ministry of Environmental Protection and Regional Development of the Republic of Latvia (Vides Aizsardzības un Reģionālās Attīstības Ministrija, VARAM), in particular Elita Zvaigzne, Arnis Skraučs, Laura Gintere, Gatis Ozols, Āris Dzērvāns, Lauris Linabergs, Mikus Jēkabsons, Uģis Bisenieks, Jānis Glazkovs, Margarita Krišlauka and Karīna Eglīte-Miezīte, as well as to Artis Grīnbergs and Prof. Edvīns Karnītis.

The Review draws on the results of a series of interviews with a wide range of stakeholders conducted during two missions to Latvia in April and December 2019, including: Ainars Andersons, Uldis Apsītis, Mikus Arājs, Armands Aivo Astukevičs, Signe Bāliņa, Dāvis Baumanis, Daiga Behmane, Edmunds Beļskis, Iveta Bērtulsone, Lāsma Dilba, Andrejs Dombrovskis, Uldis Doniņš, Oļegs Fiļipovičs, Alnis Garkājis, Jānis Grēviņš, Linda Helmane, Gundars Ignats, Aiga Irmeja, Juris Kalējs, Zita Kanberga, Inga Kasicka, Maija Katkovska, Baiba Kļaviņa, Sandis Kondrats, Katrīna Kosa-Ammari, Mārcis Kroja, Aivars Lapiņš, Artis Lapiņš, Rolands Lappuķe, Agnese Lukevica, Nellija Mahova, Juris Matvejs, Vismands Menjoks, Gatis Mezītis, Sarmīte Mickēviča, Jeļena Muhina, Vita Narnicka, Aleksejs Nipers, Laura Očagova, Jānis Paiders, Inita Pavloviča, Prof. Jurģis Poriņš, Vitālijs Rakstiņš, Zane Rozkalne, Prof. Leo Seļāvo, Kristīne Šica, Ilze Sīle, Agnese Šķēle, Ieva Skujēns-Skujiņa, Kristaps Soms, Ilze Štrassere, Renāte Strazdiņa, Rolands Strazdiņš, Elīna Stungrevica, Laura Treimane, Dainis Valdmanis, Uldis Zariņš, Olga Zeile and Sanita Žogota.

On 15 May 2020, the OECD Council invited Costa Rica to become a Member. At the time of preparation of this publication, the deposit of Costa Rica's instrument of accession to the OECD Convention was pending and therefore Costa Rica does not appear in the list of OECD Members and is not included in the OECD zone aggregates.

Table of Contents

Follow OECD Publications on:

http://twitter.com/OECD_Pubs
http://www.facebook.com/OECDPublications
http://www.linkedin.com/groups/OECD-Publications-4645871
http://www.youtube.com/oecdilibrary
http://www.oecd.org/oecddirect/

Acronyms, abbreviations and units of measure

A-Patch	Autonomous patch for real-time detection of infectious disease
ADP	Alternative dispute resolution
AHK	German-Baltic Chamber of Commerce
AI	Artificial intelligence
AIC	Availability, integrity and confidentiality
AIKA	Quality Agency for Higher Education
ALMP	Active labour market policy
ANSSI	French National Cybersecurity Agency *Agence nationale de la sécurité des systèmes d'information*
BBCE	Baltic Biomaterials Centre of Excellence
BCRD	EU broadband cost reduction directive
BIF	Baltic Innovation Fund
BIOR	Institute of Food Safety, Animal Health and Environment
BURVIS	Unemployment accounting and registered vacancy information system
CAMART	Excellence Centre of Advanced Material Research and Technology Transfer
CCC	Consumer Complaints Committee
CDU	National Guard Cyber Defence Unit
CERT	Computer emergency response team
CF	Cohesion Fund
CFCA	Central Finance and Contracting Agency
CIIT	Critical infrastructure of information technology
CISA	Cybersecurity and Infrastructure Security Agency
CISC	Cultural Information System Centre
CMS	Central Management System
CNC	Computer numerically controlled
CPB	Constitution Protection Bureau
CPEA	Consumer protection enforcement authority
CRM	Customer relationship management
CRPC	Consumer Rights Protection Centre
CSCC	Cross-Sectoral Coordination Centre
CSDD	Latvian Traffic Safety Directorate
CSIRT	Computer Security Incident Response Team
DDN	Data Driven Nation
DDoS	Distributed denial-of-service
DIH	Digital Innovation Hub
DPA	Data protection authority
DPASC	Data Protection Advisory Support Council
DRR	Dispute resolution and redress
DSB	Dispute Settlement Body
DSI	Data State Inspectorate
DSL	Domain-specific language
EAFRD	European Agricultural Fund for Rural Development
EAS	Electronic Application System
EC	European Commission
ECC-Net	Network of European Consumer Centres

ECO	Electronic Communications Office *VAS Elektroniskie Sakari*
EDPB	European Data Protection Board
EEA	European Economic Area
eIDAS	Electronic identification, authentication and trust services
EMFF	European Maritime and Fisheries Fund
ENISA	European Union Cyber Security Agency
EQAR	European Quality Assurance Register for Higher Education
ERDF	European Regional Development Fund
ERP	Enterprise resource planning
ESF	European Social Fund
ESIF	European Structural and Investment Funds
EU	European Union
EUR	Euro
FDI	Foreign direct investment
FSDI Latvia	Federation of Security and Defence Industries of Latvia
FTR	Fixed termination rate
FTTB	Fibre to the building
FTTC	Fibre to the curb
FTTH	Fibre to the home
FTTP	Fibre to the premises
GB	Gigabyte
GBP	British pound
Gbps	Gigabits per second
GDP	Gross domestic product
GDPR	General Data Protection Regulation (European Union)
GHz	Gigahertz
GPEN	Global Privacy Enforcement Network
HEI	Higher education institution
IAC	Internal Audit Council
ICME	Integrated computational materials engineering
ICPEN	International Consumer Protection and Enforcement Network
ICT	Information and communication technology
IEA	International Energy Agency
INCD	Israel National Cyber Directorate
INFSO	Information Society Development Guidelines
IoT	Internet of Things
IP	Internet Protocol
IPE	Institute of Physical Energetics
IPR	Intellectual property right
ISAC	Information Sharing and Analysis Centres
ISP	Internet service provider
IT	Information technology
IT CC	IT Competence Centre
IXP	Internet exchange point
IWC	Latvian State Institute of Wood Chemistry
JMOIC	Joint Municipality Operative Information Centre
KBC	Knowledge-based capital
KISC	Centre for Cultural Information Systems *Kultūras Informācijas Sistēmu Centrs*
LALRG	Latvian Association of Local and Regional Government

LEGMC	Latvian Environment, Geology and Meteorology Centre
LETA	Latvian Information Agency
LFICIS	Latvian Fisheries Integrated Control and Information System
LGDB	Genome Database of the Latvian Population
LIA	Latvian Internet Association
LIDA	Latvian Investment and Development Agency
LIKTA	Latvian Information and Communication Technology Association
LIX	Latvian Internet Exchange
LLKC	Latvian Rural Advisory and Training Centre
LLU	Latvian University of Life Sciences and Technologies
LMT	Latvian Mobile Telephone
LNB	Latvian National Library
LSRTC	Latvian State Radio and Television Centre
LTE	Long-term evolution
LUA	Latvian University of Agriculture
LUMIC	Microsoft Innovation Centre
LVM	Latvia's State Forests
LVRTC	Latvia State Radio and Television Centre *Latvijas Valsts Radio un Televīzijas Centrs*
M2M	Machine to machine
MB	Megabyte
Mbps	Megabits per second
MeKA	Forest and Wood Products Research and Development Institute
MFA	Ministry of Foreign Affairs
MHz	Megahertz
MIC	Microsoft Innovation Centre
MNEs	Multinational enterprises
MNO	Mobile network operator
MoA	Ministry of Agriculture
MoC	Ministry of Culture
MoD	Ministry of Defence
MoE	Ministry of Economics
MoEAC	Ministry of Economic Affairs and Communications (Estonia)
MoES	Ministry of Education and Science
MoF	Ministry of Finance
MoH	Ministry of Health
MoI	Ministry of the Interior
MoITAL	Ministry of Industry, Trade and Labour (Israel)
MoJ	Ministry of Justice
MoT	Ministry of Transport *Satiksmes Ministrija*
MoU	Memorandum of Understanding
MoW	Ministry of Welfare
Mtoe	Million tonnes of oil-equivalent
MTR	Mobile termination rate
MVNO	Mobile virtual network operator
NAF	National Armed Forces
NATO	North Atlantic Treaty Organization
NCE	National Centre for Education
NEPLP	National Electronic Mass Media Council *Nacionālā Elektronisko Plašsaziņas Līdzekļu Padome*

NGO	Non-governmental organization
NHS	National Health Service
NITSC	National Information Technology Security Council
NPI	National Industrial Policy
OECD	Organisation for Economic Co-operation and Development
OGP	Open Government Partnership
OPGW	Optical fibre ground wire
OSCE	Organization for Security and Co-operation in Europe
OSINT	Open source intelligence
OTT	Over the top
PBMTCC	Pharmacy, Biomedicine and Medical Technology Competence Centre
PDPL	Personal Data Processing Law
PIKTAPS	Public Administration Information and Communication Technology Architecture Management System
PMP	Privacy management programme
PPP	Purchasing power parity
PTAC	Authority for Consumer Rights Protection
PUC	Public Utilities Commissions
QoS	Quality of service
R&D	Research and development
RCA	Revealed comparative advantage
RE	Register of Enterprises of the Republic of Latvia
RFID	Radio-frequency identification
RIS3	National Research and Innovation Strategy for Smart Specialisation
RSU	Rīga Stradiņš University
RTU	Riga Technical University
SaaS	Software-as-a-Service
SAO	State Audit Office
SCM	Supply chain management
SEA	State Employment Agency
SEAP	Riga Smart City Sustainable Energy Action Plan for 2014-2020
SEC	Sector Expert Council
SEDA	State Education and Development Agency
SENAR	National Service for Rural Apprenticeship (Brazil)
SFSB	State Forensic Science Bureau
SIPCR	State Inspectorate for Protection of Children's Rights
SLS	State Land Service
SMEs	Small and medium enterprises
SMILE	Santa Monica Internet Local Exchange
SMP	Significant market power
SNIFFPHONE	Smart Phone for Disease Detection from Exhaled Breath
SP	State Police
SPRK	Public Utilities Commission *Sabiedrisko Pakalpojumu Regulēšanas Komisija*
SRA	Studies and Research Administration
SRDA	State Regional Development Agency
SRS	State Revenue Service
STDI	Science, Technological Development and Innovation
STEM	Science, technology, engineering and mathematics
STEP-Up	Strategies towards Energy Performance and Urban Planning
SUMMA	Scalable Understanding of Multilingual Media

UIDAI	Unique Identification Authority of India
UL	University of Latvia
UN	United Nations
USD	United States dollar
USO	Universal service obligation
VARAM	Ministry of Environmental Protection and Regional Development *Vides Aizsardzības un Reģionālās Attīstības Ministrija*
VDSL	Very high bit rate digital subscriber line
VECC	Vocational Education Competence Centres
VET	Vocational education and training
VIIS	Latvian State Education Information System
VINNOVA	Swedish Innovation Agency
VPN	Virtual private network
VPVKAC	Unified Customer Service Centres
VRAA	State Regional Development Agency
WFS	Web Feature Service
WGI	Worldwide Governance Indicators
WMS	Web Map Service
WSIS	World Summit on the Information Society

Executive Summary

Latvia has been growing fast and converging towards higher living standards since the early 2000s. However, considerable challenges lay ahead. Population size is declining fast due to aging and emigration, productivity growth declined after the 2008 global crisis and growth prospects are gloomy due to the impact of the COVID-19 pandemic.

Policies to enhance digital transformation have a key role to play in addressing these issues. *Going Digital in Latvia* examines the opportunities and challenges raised by digitalisation in Latvia, looks at current policies and makes recommendations to improve them, based on the OECD Going Digital Integrated Policy Framework. The Review also focuses on selected components of the framework according to the priorities expressed by Latvia.

Enhancing connectivity

Latvia is performing well in terms of deployment of both fixed and mobile broadband high-speed networks. However, differences in connectivity persist between urban areas and rural areas. There are also concerns about competition in the fixed broadband market, where the incumbent's share is 56%.

To be prepared for the forthcoming developments in communication technologies and markets, Latvia should:

- Evaluate the benefits of creating a convergent regulator for both telecommunication and broadcasting services.
- Establish a clear ministerial focal point for communication services.
- Simplify administrative procedures for network deployment and increase co-ordination between municipalities and the Ministry of Transport.
- Allow for a secondary spectrum market to promote more efficient use.
- Develop a comprehensive IPv6 strategy in co-ordination with all stakeholders.

Increasing adoption and use of digital technologies

Latvia has made significant progress in Internet usage in recent years, with the government now leading on digital government in Europe. Latvian people, however, remain moderate users of the Internet while businesses lag behind those in OECD countries.

Latvia should implement a coherent set of measures to:

Upgrade digital skills

- Update training under the Third Father's Son programme, provide libraries with sufficient resources for ICTs, and create a community-based ICT training programme.
- Support the development of modular programmes in higher education that include ICTs.
- Strengthen links between vocational schools and firms employing ICT specialists.
- Exempt foreign ICT specialists with proven experience, or who have completed their studies in Latvia, from labour market tests.

Increase digital uptake by firms

- Create a digital champions programme to support SMEs in sectors with low digital uptake.
- Provide consultancy and management advice to help firms catch up with highly digitised firms.
- Introduce incentives for businesses to interact with the government online.

Foster digital government

- Consolidate funding for digital government into a single ministry, which can then set priorities according to a national strategy.
- Create a civil service-wide training programme on the use of ICTs and the design of e-government services, and develop a manual of good practices.
- Promote an open data ecosystem. Establish a one-stop shop for researchers to access health and social care data.

Enhancing trust in a digital environment

Foster digital security

Latvia can build on solid foundations to address the challenges and opportunities of digital security. However, policy should better encompass the economic and social dimension of digital security, and:

- Promote the digital security strategy at the highest level of government.
- Better integrate the digital security strategy with the Information Society Development Guidelines.
- Promote upskilling and workforce-sharing programmes between public institutions.
- Enhance multi-stakeholder and international co-operation in the area of digital security, in particular with the other Baltic States.

Enhance privacy

Latvia has made significant progress in privacy and data protection though the enactment of the EU General Data Protection Regulation and the Personal Data Processing Law in 2018. However, further steps are necessary to enhance privacy:

- Provide the Data State Inspectorate (DSI) with the human and financial resources necessary to perform its tasks effectively.
- Develop DSI guidance on privacy and privacy management programmes, based on existing good international practice.
- Encourage co-operation between the DSI and other countries, for example, by joining the Global Privacy Enforcement Network.
- Establish appropriate data governance of artificial intelligence and the Internet of Things, through further collaboration with international fora such as the OECD.

Enhance consumer protection online

Latvia's consumer policy is consistent with the OECD *Recommendation of the Council on Consumer Protection in E-commerce*. The government could take further actions to:

- Enhance consumer awareness of issues associated with e-commerce.
- Improve evidence on consumer complaints related to e-commerce and assess the effectiveness of the dispute resolution and redress system.
- Enhance cross-border enforcement co-operation within and outside the European Union.

Unleashing digital innovation

Despite significant growth over the last two decades, productivity remains significantly lower in Latvia than in other OECD countries. Innovation, therefore, is key to increasing productivity and raising living standards.

To seize digital opportunities for innovation, Latvia should:

- Focus on digitalisation as a key enabler of innovation and growth.
- Promote digital innovation to address Latvia's societal and economic challenges.

- Increase research funding to ICT-related projects, including RIS3 projects.
- Raise the quality of research through competitive-based funds, higher private co-financing and systematic *ex post* evaluation.
- Assess the activities of the IT Cluster, the IT Competence Centre and other ICT-related bodies and clearly define their respective roles.

Building a whole-of-government approach

Leveraging the benefits and addressing the challenges of the digital transformation requires co-ordination across all policy domains. To help ensure a coherent and cohesive whole-of-government approach to digital transformation policies, Latvia should:

- Push digital transformation policies higher up the policy agenda.
- Define clear budget appropriations for the Information Society Development Guidelines.
- Institutionalise a co-ordination mechanism for digital transformation policies, (e.g. by investing the Deputy Prime Minister with the role of co-ordinator).

Chapter 1

LATVIA IN THE DIGITAL TRANSFORMATION: OPPORTUNITIES AND CHALLENGES

Recent economic and social trends in Latvia

Since the early 2000s, Latvia has experience rapid growth and an increase in higher living standards. Over the period 2000-19, GDP growth (3.6% a year) was among the strongest in the European Union (EU28) and much higher than the OECD average (1.8%). Unemployment has been decreasing fast from the 2010 peak (19.5%) to 6.3% in 2019, fuelling strong growth in real wages (46% over 2012-18). Despite higher unit costs, exports have increased, particularly in high-tech products.

Notwithstanding this good performance, Latvia faces considerable challenges. Its population is declining fast due to aging and emigration, contributing to skill shortages and mismatch. As in other OECD countries, productivity growth decreased after the 2008 global crisis, particularly among small firms, which account for a large share of Latvia's businesses. Growth prospects are gloomy due to the impact of the COVID-19 pandemic on the world economy (OECD, 2020a). Regional disparities in income per capita and unemployment are large while poverty remains high. Informality is widespread, holding back productivity and reducing workers' access to training.

Policies to enhance digital transformation have a key role to play in tackling these issues. Digital technologies are an enabler for innovation and productivity in firms, particularly small and medium enterprises (SMEs). Digitalisation may help foster financial inclusion and reduce informality (i.e. economic activities not covered by formal arrangements) (ILO, 2015). It can also help increase the efficiency of the taxation system, for example, by improving tax assessment and collection), thereby providing more resources for public policies. The deployment of high-speed broadband infrastructure provides the foundation for digital transformation, thus giving individuals and firms access to government services and international markets and helping to reduce regional disparities.

Online educational resources offer new tools for teaching and provide individuals and workers with opportunities for training and skills upgrading. In particular, following the closure of all schools and universities during the COVID-19 pandemic, the Latvian government has promoted distant learning to ensure continuity of schooling and to provide equal opportunities in education (Chapter 4). More broadly, the response to the pandemic has entailed a massive transition to a remote operation mode (e.g. teleworking, e-commerce, telehealth) across all economic sectors, significantly accelerating the pace of the digital transformation in Latvia.

At the same time, the digital transformation may exacerbate existing inequalities, in particular between high and low-skilled individuals, and large and small firms, as well as urban and rural regions. Policies are key here to ensure that the potential benefits from the digital transformation are shared throughout the economy and society.

The digital transformation has the potential to foster productivity

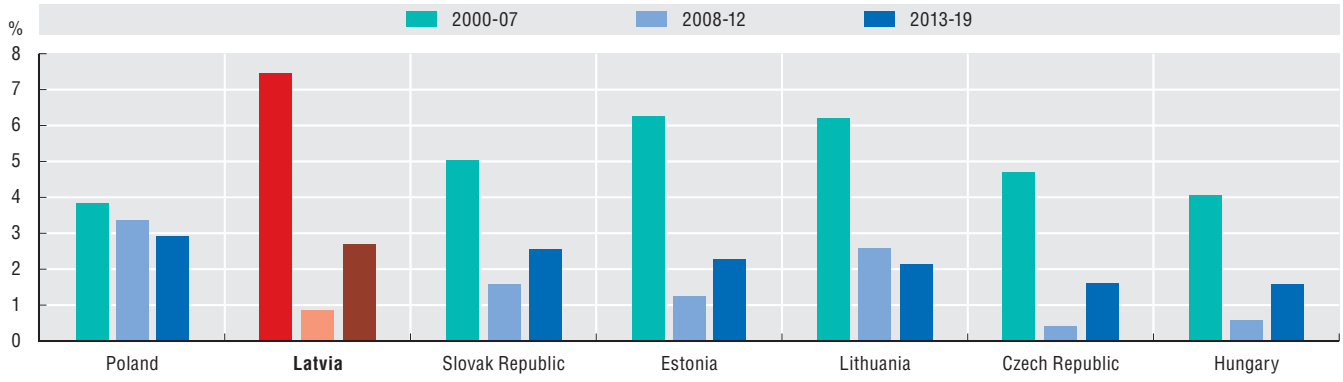
Latvia has made significant economic progress since the beginning of the millennium, with the economy growing faster than the EU28 and the OECD.[1] Over 2000-07, annual GDP growth at constant prices in Latvia was 8.5% on average, higher than in the other Baltic States (8% in Estonia and 7.6% in Lithuania) and the EU28 (2.6%). The global crisis in 2008 hit Latvia more severely than peer countries (with a contraction of -6.9% a year over 2008-10) and growth resumed at a slower pace afterwards (3.6% a year) in line with other Baltic countries but still higher than the EU28 (1.6%) (The Conference Board, 2020). The direct impact of the shutdown to contain the COVID-19 pandemic in 2020 could reduce Latvia's GDP at constant prices by 25% (OECD, 2020a).

An aging population and emigration hamper the potential for growth in Latvia. About 10% of the population emigrated between 2000-17, while the working age population (15-74 years old) dropped by 21% over the same period – the largest decrease in the OECD. In addition, drivers of growth prior to the 2008 crisis (i.e. large capital inflows, rapid debt accumulation and a real estate boom) cannot sustain future growth (Blanchard, Griffiths and Gruss, 2013), with further growth reliant on increased productivity.

Labour productivity in Latvia remains lower than in other OECD countries, providing room for improvement. In 2017, GDP per hour worked was just 54% of the hourly productivity in high-income OECD countries (OECD, 2019a). Productivity growth, however, has slowed down considerably compared to the pre-crisis period. Average yearly growth in GDP per hour worked dropped from 7.8% in 2000-07 to 2.9% in 2013-18, although it remains higher than in Baltic and Central European countries (Figure 1.1).

Figure 1.1. Labour productivity growth in Latvia and selected OECD countries, 2000-19

Average annual growth in GDP per hour worked (%)



Source: The Conference Board (2020), *The Conference Board Total Economy Database, April 2019*, *www.conference-board.org/data/economydatabase* (accessed on 6 May 2020).

Limited innovation in business seems to be an important factor in slow productivity growth. Few Latvian firms have adopted new production technologies, launched new products or introduced new organisational methods. The share of innovating SMEs is among the lowest in the OECD, with Latvian firms lagging behind other OECD countries in their use of digital technologies, which is limited to basic tools (Chapter 4).

Digital technologies have the potential to increase productivity in firms across all economic sectors. Big data and data analytics can help firms better understand their production processes, the needs of their clients and partners, and the overall business environment. Digital technologies can also improve the capability of firms to outsource key business functions and to access a range of financing instruments, which can help improve performance. Finally, online platforms can support the productivity of low-tech service firms, for example by providing them with booking facilities and efficient matching algorithms based on consumer review and rating systems (OECD, 2019b). Promoting digital uptake by businesses, particularly SMEs, would go a long way towards fostering productivity growth in Latvia (Chapter 4).

Digital innovation is key for productivity

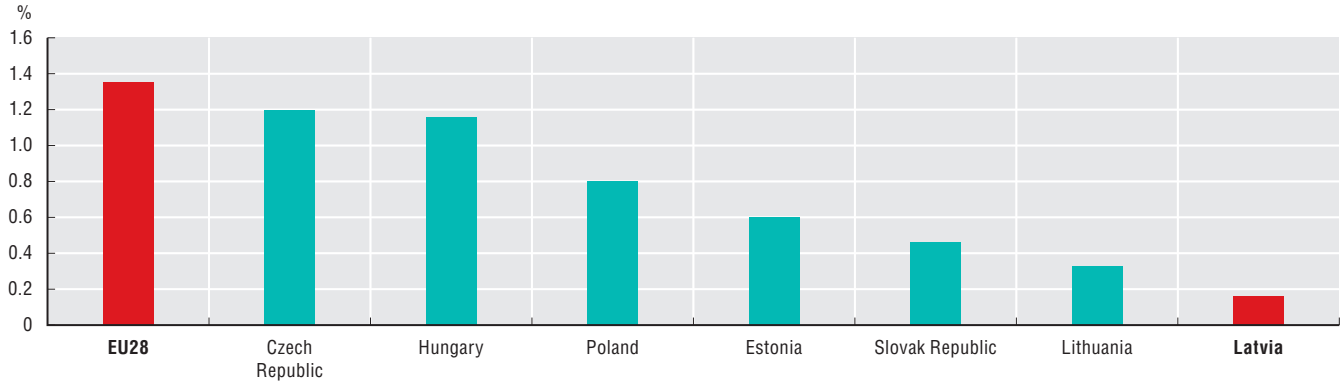
Digitalisation is opening up new opportunities for innovation. However, research and development (R&D) expenditures in Latvia are low with almost a quarter of R&D funded by the European Union. Latvian businesses also have among the lowest rates of R&D in Europe, particularly in information industries (Figure 1.2). In order to raise innovation in firms, Latvia has put in place several programmes to increase R&D as part of the National Development Plan 2014-20 (Chapter 4).

The number of researchers and PhD graduates is particularly low and incentives for higher education institutions (HEIs) to collaborate with industry seem weak, with the notable exception of Riga Technical University (European Commission, 2018a). Only 7% of Latvia's scientific publications on ICTs are listed among the top 10% of citations (OECD, 2019a). In order to improve the quality of research, the government has introduced a new funding model, concentrating resources in more effective universities and HEIs (Chapter 6).

Almost half of Latvian firms report financing as an obstacle to investment, which can act as a barrier to innovation. SME lending has remained low since the financial crisis of 2008. The Guidelines for Science, Technology Development and Innovation 2014-2020 put forward a Strategy for Smart Specialisation with the objective of fostering a structural transformation of the economy. The Strategy's key areas include a knowledge-intensive bioeconomy, biomedicine, medical technologies and biotechnology, smart materials, technology and engineering, advanced ICTs and smart energy (Chapter 6).

Figure 1.2. Business R&D in information industries[1] in Latvia and selected OECD countries, 2016

As a percentage of value added



1. "Information industries" (ISIC Rev.4) include "Computer, electronic and optical products" (Division 26), "Publishing, audiovisual and broadcasting activities" (Divisions 58 to 60"), "Telecommunications" (Division 61) and "IT and other information services" (Divisions 62 to 63).

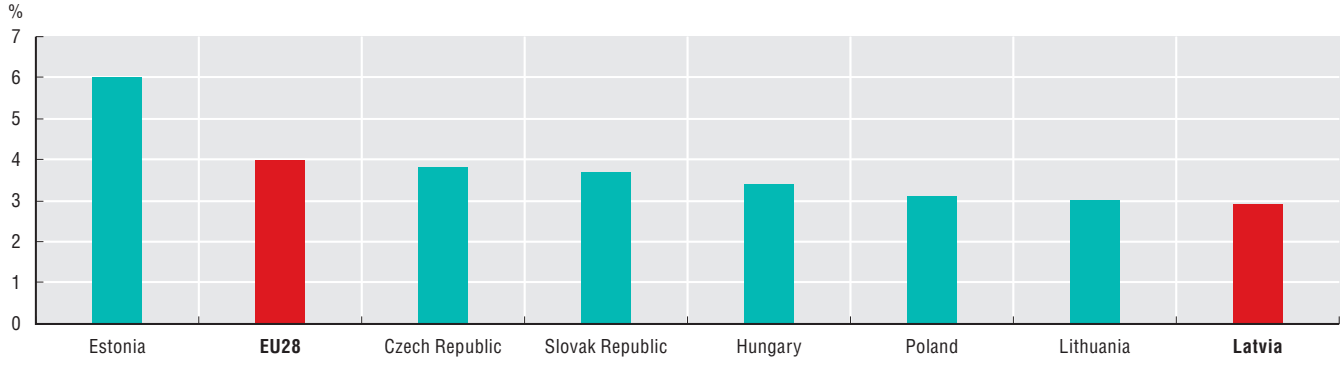
Sources: OECD (2020c), *ANBERD Database*, *http://oe.cd/anberd* (accessed on 6 May 2020); OECD (2020d), *Main Science and Technology Indicators* (database), *http://oe.cd/msti* (accessed on 6 May 2020).

Active labour market policies can help close the digital skills gap

Poor ICT skills and complementary skills such as advanced management limit the capacity of Latvian firms to make the best use of available digital technologies. For instance, over half of the population – and 67% of the unemployed – lack basic digital skills. Latvia has the lowest share of ICT specialists in employment in the European Union, with the share of women falling from 30% in 2008 to 14% in 2018 (Figure 1.3).

Figure 1.3. ICT specialists in employment in the European Union, 2018

As a percentage of total employment



Source: Eurostat (2020), *Digital Economy and Society* (database), *http://ec.europa.eu/eurostat/web/digital-economy-and-society/data/database* (accessed on 6 May 2020).

Latvian firms invest relatively little in the skills of their workers, especially with regard to ICT training. Furthermore, participation in life-long learning is low, with low-skilled workers less likely to take part in adult education. Latvia's skill shortages are exacerbated by policies that hamper the immigration of skilled workers (Chapter 4).

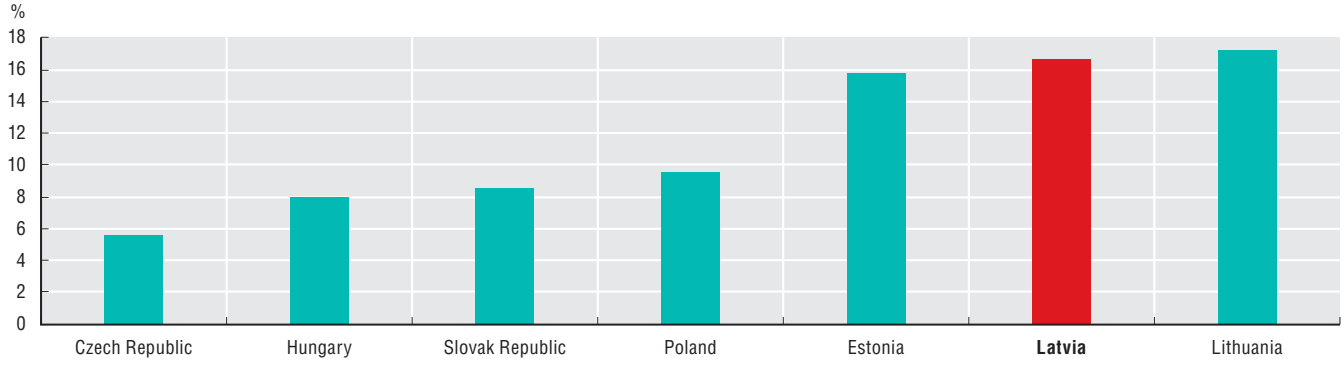
In 2016, the Latvian government spent only 0.15% of GDP on targeted training for particular groups, such as unemployed or inactive individuals or employed individuals at risk of involuntary job loss. This compares to 0.21% in Estonia, 0.24% in Lithuania and 0.36% across the OECD (OECD, 2018a). While the training system for unemployed workers and activation policies have improved in recent years, there is room for Latvia to foster skills for digitally intensive jobs by increasing public spending on active labour market policies (Chapter 4).

Using digital tools to foster inclusive growth

Overall living standards have improved fast in Latvia during the last two decades, but poverty remains higher than in other OECD countries (Figure 1.4). Reforms in 2018 made personal income taxes more progressive but tax revenues as a share of GDP are well below the OECD average. In particular, tax revenue losses due to widespread informality limit the government's ability to invest in infrastructure and social services (OECD, 2019a).

Figure 1.4. Individuals living in poor households in Latvia and selected OECD countries, 2017

As a percentage of total population



Note: The poverty threshold is 50% of median household disposable income. Household income is adjusted to take into account household size.

Source: OECD (2020e), *Income Distribution Database (IDD)*, *http://oe.cd/idd* (accessed on 6 May 2020).

Digital technologies can help strengthen the enforcement of tax and labour laws. The use of algorithms to analyse the data collected by the tax administration can improve the detection of tax evaders (OECD, 2018b), while better information exchange between law enforcement agencies would contribute to increasing their effectiveness. Latvia's State Revenue Service (SRS) is implementing digital tools and data analysis systems to better target audits at high-risk taxpayers. SRS is also working on a system to automatically match data received from foreign tax authorities with domestic data. By raising trust in public institutions, open government data can help fight informality and improve compliance with tax laws (Mickiewicz, Rebmann and Sauka, 2019). Digital job platforms could help boost labour market formality, formalise word-of-mouth transactions and allow tax authorities to extract data from such transactions, provided that appropriate regulations are in place.

Regional disparities in income per capita and unemployment are pronounced, leading to large differences in per capita tax revenues among municipalities. In addition, municipalities in Latvia are relatively small, which undermines the provision of high-quality public services, including education and public transport. Merging small municipalities would help to consolidate resources but is politically difficult. Digitalisation provides an opportunity to pool digital resources and e-services among several municipalities, helping to improve the efficiency of local public service provision and reduce the growing urban-rural divide.

Together with better transport infrastructure, high-speed broadband and better use of digital technologies would create economic opportunities for workers and businesses, particularly SMEs, in disadvantaged regions (Chapter 3).

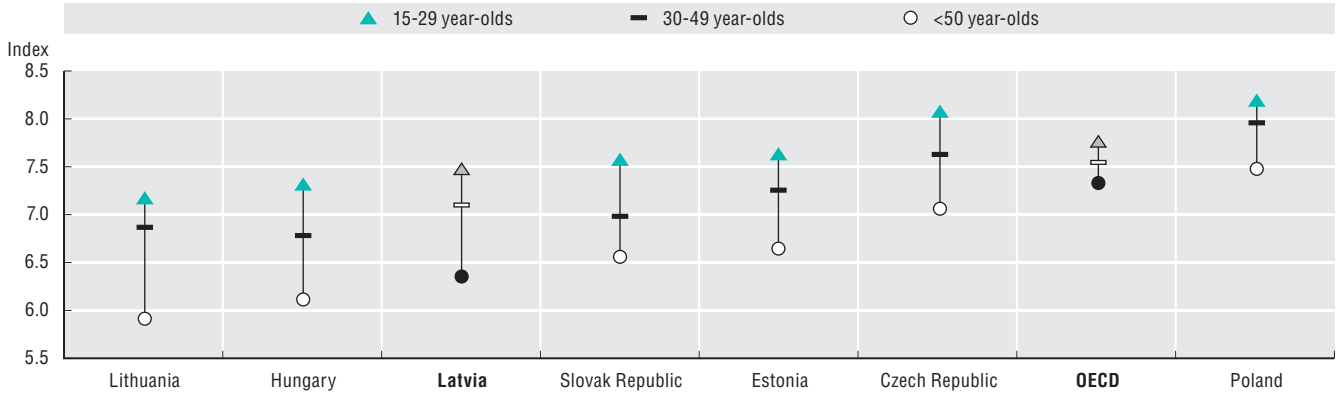
Enhancing well-being along the digital transformation

While average living standards have been steadily improving in Latvia, progress in well-being has been slower, particularly for certain groups. In 2017, 74% of the poorest households (bottom income quintile) in Latvia regarded their health as bad/very bad or fair, against 36% in the richest households (top income quintile). Not only was this gap (38 percentage points) much higher than the OECD average (21 percentage points), it has widened by over 10 percentage points since 2010 (OECD, 2020b).

Life satisfaction remains particularly low among elderly people (50+), with an index value of only 6.3 (on a scale of 10) compared to the OECD average of 7.3 (Figure 1.5). Across age groups, Latvia also has among the highest number of deaths from suicide and substance abuse, largely related to alcohol (OECD, 2020b).

Figure 1.5. Life satisfaction in the OECD, 2018

Mean values of life satisfaction on a 0-10 scale, by age group



Note: For detailed figure notes, see: *https://doi.org/10.1787/888934081815*.

Source: OECD (2020b), "Evaluating the initial impact of COVID-19 containment measures on economic activity", *https://oe.cd/il/2VU*.

Targeted digital inclusion policies (e.g. the Third Father's Son programme) as well as further development of distant learning following the COVID-19 shutdown (Chapter 4), are crucial to closing the digital divide. Further development of e-health can improve access to health care for households in remote areas as well as to community-based services or home care in urban areas.

Finally, digital transformation can help in tackling collective challenges, including environmental management and protection (OECD, 2019b). Economic progress has increased the material footprint per capita in Latvia by over 3 tonnes since 2010 (OECD, 2020b). Digital technologies can enhance production efficiency and reduce material waste, thus improving sustainability while simultaneously increasing living standards. Smart materials, smart engineering and Smart Cities hold significant potential to enhance energy efficiency and foster the development of new environmental technologies (Chapter 6).

The Latvian Digital Transformation Strategy

The Information Society Development Guidelines 2014-2020 (INFSO) lay down Latvia's digital strategy (Chapter 7). The Guidelines are a medium-term development plan, developed by a working group co-ordinated by the Ministry of Environmental Protection and Regional Development, and consisting of representatives from 12 sectoral ministries as well as several other public and private stakeholders, including ICT associations, chambers of commerce, local and regional governments (Cabinet of Ministers, 2013a).

INFSO 2014-2020 builds on the assessment of INFSO 2006-13. While Latvia achieved the objectives for Internet access and ICT usage set out in INFSO 2006-13, it lagged behind in terms of the size of the ICT sector and the use of e-commerce by both businesses and individuals, with overall e-health uptake still unclear due to lack of statistics. In addition, despite great progress over the 2006-13 period, there remains significant untapped potential for digital government, particularly in relation to internal process optimisation.

The aim of INFSO 2014-2020 is "to provide an opportunity for everyone to use the possibilities offered by ICT, to develop a knowledge-based economy and to improve the overall quality of life by contributing to the national competitiveness, and increasing and economic growth and job creation" (Cabinet of Ministers, 2013a).

Economic growth and job creation are at the core of the strategy and inform the formulation of each of the seven action plans outlined in the guidelines: 1) ICT education and skills; 2) widely available access to the Internet; 3) advanced and effective public administration; 4) e-services and digital content for the public; 5) cross-border co-operation for the Digital Single Market; 6) ICT research and innovation; and 7) trust and security. Each action plan incorporates several components, as shown in Table 1.1.

Table 1.1. Information Society Development Guidelines 2014-2020: Action directions

Action directions	Components
ICT education and skills	Public awareness and readiness to use e-opportunities
	Development of citizen and entrepreneur e-skills
	Increase in public administration ICT competences
	Training of ICT practitioners and professionals according to labour requirements
	Promotion of algorithmic thinking and information literacy in educational programmes
Widely available access to the Internet	Transport networks
	Last mile
	Grids
	Mapping the current electronic communications network infrastructure
Advanced and effective public administration	Modernisation of basic public administration processes and activities
	Public e-participation and e-democracy
	Single public administration data space
	Optimisation of ICT infrastructure
E-services and digital content for the public	Opening of public administration data and transaction services to other users
	Development of shared platforms and services for the provision of public services
	Introduction of official e-mail addresses for citizens and entrepreneurs
	Digitalisation of public services
	Automated issuing and acceptance of electronic invoices
	Digitalisation and availability of cultural heritage
	Stimulation of Latvian language usage in the digital environment
	E-health solutions for efficient, safe and patient-oriented health care
Cross-border co-operation for the Digital Single Market	Creation of cross-border e-services and data exchange solutions
	Development of basic solutions for the provision of cross-border services
ICT research and innovation	ICT research
	Innovation
Trust and security	ICT security
	Human safety
	Trust in the electronic environment

Note: ICT = information and communication technology.

Source: Cabinet of Ministers (2013b), *Organisational Model for the Management of Public Information and Communications Technologies*, *www.varam.gov.lv/in_site/tools/download.php?file=files/text/Darb_jomas/elietas//E2269_Organisational_Model_for_the_Management_of_Public_Infor_and_Com_Techn.doc*.

INFSO 2014-2020 devotes special attention to the use of open data principles in public administration, as a tool to improve efficiency in public service delivery. Upgrading e-skills and improving Internet access and speed also have a prominent role, as enablers for e-commerce and e-business. The use of digital tools to reduce the administrative burden for business, notably SMEs, and improve the efficiency of the public administration is also key to INFSO 2014-2020.

A progress assessment of implementation of the guidelines was completed in October 2019 (VARAM, 2019). The final assessment will be submitted to the Cabinet of Ministers by the Ministry of Environmental Protection and Regional Development in July 2021.

Several other development documents are currently being implemented, several of which have a focus on improvement of e-government services. They include the Organisational Model for the Management of Public Information and Communications Technologies (Cabinet of Ministers, 2013b), the Conceptual

Architecture of Public Administration Information Systems (Cabinet of Ministers, 2015), and the information reports Using Cloud Computing Services in Public Administration (Cabinet of Ministers, 2018) and Latvia's Open Data Strategy (Cabinet of Ministers, 2019) (Chapter 4), as well as the Information Report on the Development of Artificial Intelligence Solutions (Cabinet of Ministers, 2020).

Other documents, such as the Concept for the Development of Next Generation Broadband Electronic Communications Networks 2013-2020 and the Electronic Communications Policy Plan 2018-2020, focus more on ICT access and infrastructure (Chapter 3). To these can be added the Guidelines for the Protection and Enforcement of Intellectual Property Rights 2015-2020, as well as the Cyber Security Strategy of Latvia 2014-18. Latvia's Cyber Security Strategy 2019-2022 was approved in September 2019 (Chapter 5).

Latvia does not currently have an overarching strategy in place for the digitalisation of business. There is, however, a Smart Specialisation Strategy, which is flanked by the Science, Technological Development and Innovation Guidelines for 2014-2020 (STDI) and the National Industrial Policy (NPI) guidelines 2014-2020. The latter aim explicitly to promote the modernisation of industry (European Commission, 2018b). The NPI were presented in 2012 and aim, among other objectives, to align workforce supply and education to the needs of economic development and to promote an open, creative and innovative environment. The NPI objectives were further articulated by the Programme for Improvement of the National Innovation System, approved by the National Strategic Council for Research and Innovation in 2016 (Chapter 6).

The Going Digital Integrated Policy Framework

As pointed out in Latvia's Information Society Development Guidelines, digital transformation affects different parts of the economy and society in complex and interrelated ways, making trade-offs between public policy objectives difficult to navigate.

The OECD has developed an integrated policy framework to support a whole-of-government approach to coherent policy making in the digital age. The framework recognises technologies, data and business models as driving forces underlying digital transformation, and considers the transformation across many different policy areas. The framework itself includes seven integrated building blocks (Figure 1.6).

Figure 1.6. Going Digital Integrated Policy Framework

Source: OECD (2019b), *Going Digital: Shaping Policies, Improving Lives*, *https://doi.org/10.1787/9789264312012-en*.

These integrated building blocks do not represent discrete policy domains; rather, each brings together multiple policy areas (see below for more details). This configuration underscores the point that leveraging the benefits and addressing the challenges of digital transformation requires identifying policy areas that are jointly affected and require co-ordination. It further implies that all building blocks are needed to make digital transformation work for growth and well-being.

Going Digital in Latvia aims to help Latvia ensure a coherent and cohesive whole-of-government approach to better respond to digital transformation and make it work for growth and well-being.

Access

Reliable communications infrastructure and services underpin the use of all digital technologies, and facilitate interactions between connected people, organisations and machines. Similarly, the data that flow through networks are also emerging as a source of value in the digital era, although their productive use is predicated on their availability.

As reliable communications infrastructures and services are essential to digital transformation, the first integrated building block concerns access to data, communications infrastructures and services (e.g. fibre optic backhaul, towers, spectrum, international cables). This encompasses efficient, reliable and widely accessible broadband communication networks and services, and key complementary enablers (e.g. a co-ordinated system of international domain names, increasing uptake of IPv6 Internet addresses, Internet exchange points [IXPs]), data, software and hardware. These components together act as the technical foundation for an open, interconnected and distributed Internet that enables the global free flow of information and, more generally, digital transformation. Multiple policy domains need to be considered to ensure access, including communications infrastructures and services, competition, investment and regional development.

Use

Access to digital networks provides the technical foundation for the digital transformation of economy and society. However, such access does not necessarily ensure the widespread diffusion of digital tools and their effective usage, which are necessary for individuals, governments and firms to reap the benefits of digital transformation through increased participation, innovation, productivity and well-being. Diffusion and effective use depend crucially on a number of variables including: investment in ICTs and knowledge-based capital (KBC), including data and organisational change; a favourable business environment (e.g. one that fosters business dynamism); the availability and allocation of skills; and trust. Multiple policy domains must therefore be considered, notably digital government, investment, business dynamism and SMEs, education and skills, and digital security and privacy.

Innovation

Innovation pushes the frontier of what is possible, driving job creation, productivity growth, and sustainable growth and development. Digital innovation, in particular, has driven radical changes in the ways that people interact, create, produce and consume. Digital innovation not only gives rise to new and novel products and services, but also creates opportunities for new business models and markets, and can drive efficiencies in the public sector and beyond. In addition, digital technologies and data drive innovation in a wide range of sectors, including education, health, finance, insurance, transportation, energy, agriculture and fisheries, as well as the ICT sector itself. Multiple policy domains need to be considered in order to foster innovation, including entrepreneurship and SMEs, science and technology, competition, digital government, and sectoral policies such as energy, finance, transport, health and education, among others.

Jobs

Digital transformation has already begun to change the nature and structure of organisations and markets, raising important questions about which jobs might disappear and where new ones will arise, what they will look like and which skills will be required. At the same time, issues around who might

be most affected, and what can be done to foster new job creation and align skills development with the changing skills requirement of jobs, have emerged. Technological advances and the introduction of new business models have given rise to the "platform economy" and led to the emergence of new forms of work such as "crowd work", "gig work" and other forms of on-demand labour. Ensuring that digital transformation leads to more and better jobs will depend on the kind of policies put in place, especially in the areas of labour markets, education and skills, and social protection. As impacts may be concentrated in certain industries and regions, sectoral and regional policies will also play an important role.

Society

Digital transformation affects society and culture in complex and interrelated ways, as digital technologies change the ways in which individuals, firms and governments interact among and with one another. For digital transformation to enhance growth and well-being, it is essential that public policies support a positive and inclusive digital society. To do so, multiple policy domains need to be considered, including social policies (e.g. housing and welfare), education and skills, tax and benefit policies, environment, health and digital government. Digital transformation changes the distribution of benefits, raising questions about where life is getting better, and for whom, and making social policies an important part of the policy toolbox, able to address a range of digital divides.

Trust

Trust is fundamental to the digital transformation. In its absence, individuals, firms and governments will not make full use of digital technologies, and an important source of potential growth and social progress will remain unexploited. Countries may benefit from greater cross-border co-operation if they develop comprehensive and coherent national strategies for digital security and privacy to address issues such as the protection of personal data, the resilience of essential services (e.g. water, energy, finance, public health and safety), the creation of incentives (e.g. cyber insurance, public procurement), support to SMEs, and related skills development in consultation with all relevant stakeholders. At the same time, it is important to continue promoting effective protection to consumers engaged in e-commerce and other online activities, as this will help the digital economy flourish and become more inclusive.

Market openness

Digital technologies are transforming the environment in which firms compete, trade and invest. Market openness policies related to trade, investment, financial markets, competition and taxation play an important role in ensuring that favourable conditions exist for the digital transformation to flourish. Digital transformation also affects policies related to market openness, raising opportunities and posing challenges. Governments could benefit from periodically reviewing their market openness policies and, where appropriate, updating them to ensure they are well suited to making digital transformation work for growth and well-being.

Going Digital in Latvia

The Review is organised as follows:

Chapter 2 uses strategic foresight to explore three alternative future scenarios, which could result from the present digital transformation of the global economy and society. These foresight scenarios are intended to help Latvian decision makers better anticipate disruptive changes, identify critical uncertainties, develop innovative new strategies and policies, and stress-test existing plans and practices.

Chapter 3 reviews recent developments in the Latvian communication market, examines institutional frameworks as well as communication policies and regulation, and provides policy recommendations.

Chapter 4 reviews recent trends in the use of digital technologies by individuals, businesses and the government in Latvia. It examines national programmes to overcome digital divides among individuals and firms, and provides policy recommendations, including for the development of digital skills.

Chapter 5 analyses Latvia's digital security policies to foster economic growth and resilience, examines the steps taken to ensure that people can trust that their data are managed in a confidential manner and their privacy is protected, reviews the Latvian framework for protecting digital consumers and provides policy recommendations to enhance trust in the digital economy in Latvia.

Chapter 6 reviews the main technological trends driven by digitalisation, including R&D and big data. It examines Latvia's innovation policies in this area and makes recommendations for promoting digital innovation in the national innovation system. It also reviews recent transformations in Latvia's key industries and services and examines national policies with a view to fostering "smart" specialisations, particular in relation to Latvia's integration in global value chains.

Chapter 7 examines the policies analysed in the previous chapters in relation to their coherence among different domains, and provides recommendations to foster synergies across government ministries, levels and institutions, based on the OECD Going Digital Integrated Policy Framework.

References

Blanchard, O., M. Griffiths and B. Gruss (2013), "Boom, bust, recovery: Forensics of the Latvia crisis", *Brookings Papers on Economic Activity, Economic Studies Program*, Vol. 44, pp. 325-388.

Cabinet of Ministers (2020), Informatīvais ziņojums "Par mākslīgā intelekta risinājumu attīstību" [Information report "On the development of artificial intelligence solutions"], Riga, *http://tap.mk.gov.lv/doc/2020_02/IZ_MI%5b1%5d.2.docx*.

Cabinet of Ministers (2019), *Latvijas atvērto datu stratēģija* [Latvia's Open Data Strategy], Riga, 20 August, *http://polsis.mk.gov.lv/documents/6533*.

Cabinet of Ministers (2018), *Mākoņdatošanas pakalpojumu izmantošana valsts pārvaldē* [Using Cloud Computing Services in Public Administration], Riga, 20 February, *http://polsis.mk.gov.lv/documents/6140*.

Cabinet of Ministers (2015), *Informatīvais ziņojums "Par publiskās pārvaldes informācijas sistēmu konceptuālo arhitektūru"* [Information Report "On the conceptual architecture of public administration information systems"], Riga, 10 March, *http://tap.mk.gov.lv/mk/tap/?pid=40338790*.

Cabinet of Ministers (2013a), *Information Society Development Guidelines 2014-2020 – Informative Part*, Order No. 486, Riga, 14 October, *www.varam.gov.lv/in_site/tools/download.php?file=files/text/Darb_jomas/elietas//Information_Society_Development_Guidelines_2014_2020.docx*.

Cabinet of Ministers (2013b), *Organisational Model for the Management of Public Information and Communications Technologies,* Order No. 57, Riga, 15 January, *www.varam.gov.lv/in_site/tools/download.php?file=files/text/Darb_jomas/elietas//E2269_Organisational_Model_for_the_Management_of_Public_Infor_and_Com_Techn.doc*.

European Commission (2018a), *The Latvian Research Funding System*, European Commission Directorate-General for Research and Innovation, Brussels, *https://rio.jrc.ec.europa.eu/en/library/specific-support-latvia-final-report-%E2%80%93-latvianresearch-funding-system*.

European Commission (2018b), *Digital Innovation Hubs – Smart Specialisation Platforms*, Brussels, *https://s3platform.jrc.ec.europa.eu/digital-innovation-hubs-tool/-/dih/13295/view* (accessed in February 2020).

Eurostat (2020), *Digital Economy and Society* (database), *http://ec.europa.eu/eurostat/web/digital-economy-and-society/data/database* (accessed on 6 May 2020).

ILO (2015), *Recommendation No. 204 concerning the Transition from the Informal to the Formal Economy*, Meeting document, *www.ilo.org/ilc/ILCSessions/previous-sessions/104/texts-adopted/WCMS_377774/lang--en/index.htm*.

Mickiewicz, T., A. Rebmann and A. Sauka (2019), "To pay or not to pay? Business owners' tax morale: Testing a neo-institutional framework in a transition environment", *Journal of Business Ethics*, Vol. 157, pp. 75-93, *https://link.springer.com/article/10.1007/s10551-017-3623-2#article-info*.

OECD (2020a), *How's Life? 2020: Measuring Well-Being*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9870c393-en*.

OECD (2020b), "Evaluating the initial impact of COVID-19 containment measures on economic activity", OECD, Paris, *https://oe.cd/il/2VU* (accessed on 28 May 2020).

OECD (2020c), *Analytical Business Enterprise Research and Development (ANBERD) Database*, OECD, Paris, *http://oe.cd/anberd* (accessed on 6 May 2020).

OECD (2020d), *OECD Main Science and Technology Indicators (MSTI)* (database), OECD, Paris, *http://oe.cd/msti* (accessed on 6 May 2020).

OECD (2020e), *OECD Income Distribution Database (IDD)*, OECD, Paris, *http://oe.cd/idd* (accessed on 6 May 2020).

OECD (2019a), *OECD Economic Surveys: Latvia 2019*, OECD Publishing, Paris, *https://doi.org/10.1787/f8c2f493-en*.

OECD (2019b), *Going Digital: Shaping Policies, Improving Lives*, OECD Publishing, Paris, *https://doi.org/10.1787/9789264312012-en*.

OECD (2018a), "How does Latvia compare?" *The New OECD Jobs Strategy: Good Jobs for All in a Changing World of Work*, OECD, Paris, *www.oecd.org/latvia/jobs-strategy-LATVIA-EN.pdf*.

OECD (2018b), *Tax Challenges Arising from Digitalisation – Interim Report 2018: Inclusive Framework on BEPS, OECD/G20 Base Erosion and Profit Shifting Project*, OECD Publishing, Paris, *http://dx.doi.org/10.1787/9789264293083-en*.

The Conference Board (2020), *The Conference Board Total Economy Database, April 2019*, *www.conference-board.org/data/economydatabase*.

VARAM (2019), *Informācijas sabiedrības attīstības pamatnostādņu 2014. – 2020. gadam starpposma 2. Izvērtējums* [2nd Interim Evaluation of the Information Society Development Guidelines 2014-2020], Ministry of Environmental Protection and Regional Development, *http://polsis.mk.gov.lv/api/file/file7299860066764117769.pdf*.

Note

1. The comparisons given in this report do not aim to benchmark Latvia against a given set of countries, but to understand Latvia's performance in different policy areas related to digital transformation. Therefore, the countries/regions considered for the comparison may vary from one area to another.

Chapter 2

KEY FUTURE UNCERTAINTIES IN DIGITAL TRANSFORMATION AND POTENTIAL IMPLICATIONS FOR LATVIA

Introduction

Digital transformation is driving rapid change on an unprecedented global scale, generating heightened uncertainty. In this context, individuals, organisations and governments planning for upcoming decades can no longer rely on assumptions that the future will resemble the present to any great extent. Rather, they must explore and prepare for a range of alternative scenarios embodying potential changes and the new opportunities and challenges they might bring. Such an approach can help ensure that the strategies and policy frameworks designed today are resilient and adaptive in the face of digital transformation and the direction, pace and scale of changes it could bring.

This chapter begins by exploring three alternative scenarios for the future of digital transformation, based on broad differences in power structures and relationships between societal actors. The first scenario considers a world where active citizens take digitalisation into their own hands and form a comprehensive "third pillar" of empowered online communities that provide a counterweight to states and markets. The second scenario describes a world in which governments set up digital platforms that become the backbone of their economies, promoting exchange between countries using the same system but creating barriers with those who do not. The third scenario presents a future in which multinational digital corporations become so efficient and comprehensive in serving their users that many of the roles traditionally held by the state, such as education and welfare, are offered by non-state entities.

Individually, and as a set, these scenarios provide an opportunity to rethink untested assumptions about future trajectories and the policies built on them. What roles might communities and peer-to-peer initiatives play in Latvia's digital future? What kind of digital government does Latvia want to be? In which strategic partnerships and collective initiatives might Latvia participate to secure its place in the world? Scenarios in themselves do not provide answers to these questions, but rather provide a framework within which such questions can be asked.

The chapter concludes by identifying some key perspectives for action that emerge from the scenario analysis. These actions fall into four main categories: 1) evaluating and strengthening Latvia's strategic partnerships for digital transformation; 2) identifying smart approaches to education and skills for adaptive and critical Latvians; 3) finding pathways to an inclusive digital Latvia, by and for the people; and 4) building capacity to benefit from the access and use of personal data while safeguarding digital security and privacy.

Why scenarios? Decision making in a context of uncertainty

The pace and scale of digital transformation is creating a high level of uncertainty regarding the shape of the future in the coming years. As a range of linked digital technologies continue to emerge and combine, enabling radical new actions and behaviours, these in turn produce cascading and uncertain implications for all aspects of society, the economy, environment and governance. Unlike more predictable global megatrends, such as population aging, which may take place gradually over decades, technological change can lead to sudden and divergent impacts that are difficult to anticipate.

It is impossible to predict or fully control which new business models may emerge, which new forms of collective action may be enabled, which digitally powered forms of state involvement may prove most effective, how the structure and functioning of the economy may evolve, and how the changing nature of value and power in a more digital world may reshape the global order. With each of these uncertainties come potential changes that could bring tremendous opportunities to improve human well-being and address complex global challenges, but could also generate significant disruption and create new potential threats.

Designing effective strategies and policies in a fast-moving and unpredictable domain such as digital transformation demands a strategic foresight approach (Box 2.1). This entails looking beyond current trends and expectations about the future and considering a number of different scenarios. Foresight

scenarios are a set of alternative descriptions of how the future might look, constructed for the purpose of taking action in the present. They are not forecasts or an attempt to predict what the future will look like. Neither are they a set of recommendations or vision of any particular desired future. Put simply, scenarios do not say what *will or should* happen; only what *might* happen, leaving the question what can be learned from them open to discussion.

The foresight scenarios presented in this chapter are intended to help Latvian decision makers better anticipate disruptive changes, develop innovative new strategies and policies, and test existing plans and practices against a range of plausible alternatives. Additional benefits from using scenarios in policy making include the ability to reveal and test implicit assumptions about the future in current policy, to connect policy domains previously separated into silos, to turn disagreement among experts into an asset and to discuss matters that might otherwise be too sensitive to raise.

The scenarios were produced using the outputs of an initial one-day foresight workshop that brought together a wide range of Latvian stakeholders working in the fields of policy, technology academia and others. The scenario exercise also incorporated findings from a series of interviews with Latvian policy makers and experts, a foresight survey, an OECD internal scenarios exercise, and inputs from the OECD Directorate for Science, Technology and Innovation. Two additional foresight workshops were then held to refine the policy implications brought forward at the end of this chapter and to identify crucial issues for Latvia's digital future.

Box 2.1. What is strategic foresight?

Strategic foresight is a discipline that looks beyond current assumptions and, instead, takes into account a range of plausible future developments with a view to identifying implications for policy making. It employs a range of methodologies, such as scanning the horizon for emerging changes, analysing megatrends and developing multiple scenarios.

Strategic foresight can assist governments in designing **more resilient and adaptive strategies** through the following approaches:

- **Better anticipation** identifies changes that could emerge in the future and new opportunities and challenges for policy making.
- **Future-proofing** uses a range of plausible future scenarios to stress-test existing strategies.
- **Policy innovation** develops new innovative ideas and policies that are robust across a range of futures.

How to use this chapter

This chapter is intended as a starting point for further analysis and deliberation on the future of digital transformation and potential implications for Latvia. Its findings, while largely consistent with the rest of this report, can also be viewed as complementary, and can serve as an additional lens to evaluate how best to implement the recommendations contained in other chapters, in particular where these might be affected by unexpected future developments.

Above all, it is hoped that this chapter will serve as an inspiration and building block for ongoing strategic foresight dialogue in Latvia. This entails modifying the scenarios and developing new ones as circumstances evolve, as well as exploring the deeper intersections of digital transformation with other key sources of disruption, such as COVID-19 (Box 2.2). Such sustained and participatory strategic foresight efforts by Latvia's decision makers and the broader policy community will be indispensable to the ongoing work of developing resilient and adaptive strategies for Latvia's success in the digital era.

Box 2.2. Implications of the COVID-19 pandemic

The sudden emergence of the COVID-19 global pandemic provides a clear reminder of the importance of preparing for the unexpected. Although the likelihood of such a pandemic had long been accepted, its precise timing and nature have been unpredictable. The pandemic is now generating further cascading waves of disruption and uncertainty affecting all areas of policy. In this context of heightened turbulence, strategic foresight approaches, such as the one demonstrated in this chapter, can help governments avoid the risk of making policy decisions based on overly hasty or narrow assumptions about the future.

Some interactions between COVID-19 and digital transformation already seem clear, including a sudden acceleration of online work, learning, commerce, entertainment and politics. The uncertainties, however, are even greater. For example, will there be a lasting growth in virtual work, and how might this affect earnings and migration patterns both within and between countries? Will COVID-19 hasten deglobalisation and the creation of separate digital regions, or create momentum for renewed global collaboration? Will the economic crisis increase the dominance of large technology firms or create new niches for innovative competitors? Will citizens welcome or reject new forms of digital surveillance aimed at advancing public health? Could concerns over increasing sovereign debt lead to a growth of cryptocurrencies? What kinds of digitally enabled political movements might emerge as a result of the social fractures accentuated by the crisis?

While this chapter was drafted before the emergence of the COVID-19 pandemic, the three scenarios described can serve as a valuable foundation for thinking through many of the further uncertainties and possible developments related to the interactions between COVID-19 and digital transformation, and the potential implications for Latvia's digital strategy.

Directions for a desirable digital Latvia

The ultimate purpose of the strategic foresight analysis in this chapter is to help Latvia identify pathways towards a desirable digital future, while consciously navigating a context of uncertainty. In order to create a basis for this discussion, the workshops included an exchange on overarching priorities and aspirations for the country's digital future. These should not be considered a formal consolidated government vision, or the official position of any individual or organisation. Rather, they capture some insights into future directions that were perceived favourably by Latvian stakeholders and policy makers alike. During the intervention, these directions served as a first step towards identifying strategic options for the government to consider. They represent a starting point for discussion, setting a basis for a fruitful debate on Latvia's ambitions and priorities going forward.

Stakeholders and policy makers both voiced their desire for an inclusive digital Latvia for and by the people. This would imply putting the well-being of Latvians at the centre of any decision, programme or policy objective, and giving Latvian citizens a chance to connect, contribute and be digitally active. Latvians have expressed a desire for a digital future where they can participate in their own language and in line with their individual capabilities and limitations. This aspiration carries the need to create digital opportunities for all and ensure that Latvians have the necessary skills and tools to make use of them to their best advantage. Stakeholders wish to be involved and be given the chance to contribute to Latvia's digital transformation. One way to allow the voices of citizens to be heard would be public consultations on digital topics.

Closely linked to this aspiration is the desire for a successful digital Latvia to be based on a smart approach to education and skills. This includes an adaptive and responsive education sector that fosters digital learning for all Latvians, both in the form of generic ICT skills (digital literacy and data literacy) as well as complementary skills such as information processing and problem-solving capacities. A digitally skilled nation is one where citizens in urban and rural areas alike can benefit from digital opportunities and know how to safeguard themselves in digital environments. It is one in which learning systems at all levels have the capacity to adapt and evolve with their environment, responding to market needs and technological development. It also works to fully harness the rapidly

improving opportunities for life-long learning outside the formal education system, made possible by technological advances, for example learning by doing at work and in daily life. Smart education would allow for existing knowledge and expertise to spread and for new partnerships to form and flourish. In Latvia, digital skills should not be considered in isolation, but rather be closely connected to people's personal and professional ambitions, and seen as a means to enhance the human capital of all citizens.

Another aspiration for Latvia's future is to create a sense of connectedness by strengthening the country's internal co-operation and networks. Stakeholders and policy makers alike voiced the wish for greater collaboration between public, private, civil society, academic and individual actors, in order to better connect existing capabilities. Moving from shorter-term, project-based agreements towards more long-term partnerships in various fields could allow for even more stable relationships to develop. These partnerships might exceed the purpose of knowledge exchange, creating a productive environment where innovation can flourish. Strategic connections between the myriad successful projects in the digital field would strengthen Latvia's position as a small and flexible country. This approach could also offer opportunities to serve as a test bed for new public-private partnership concepts.

A further desired aspect of Latvia's digital success is the ongoing capacity to safeguard digital security and safety. This means enabling Latvians to use technologies in a safe and protected manner, while allowing them to share data openly. Rapidly evolving conditions require constant strengthening of digital security and ethics safeguards, built systematically into decision-making processes. The desired result would be the successful integration of digital systems with both individual and institutional security a priority.

Three scenarios: Imagining Latvia in various future contexts

The three scenarios below provide alternative descriptions of future environments that Latvia could face in the coming years. These scenarios are intentionally extreme, fictional simplifications intended as a tool for identifying potential new opportunities and challenges. None of these scenarios will come about as described and the truth is likely to be a messy combination of all three as well as other factors. The state of the Latvian society and economy in each of the scenarios can only be imagined – and will depends on a range of interconnected (re)actions and developments, as well as various policy choices over the course of many years. Nonetheless, it is possible to envisage certain characteristics of each of the "future Latvias", pointing towards challenges the country may face as well as opportunities it can seize.

#Me2.0

People have harnessed digital technologies to create new regional and global communities to better advance their interests.

These movements have challenged the dominance of governments and firms, forming a third pillar of the global system: the civil sector.

Communities use technologies effectively to tackle local and global challenges.

Polarisation between groups and questions of accountability remain challenging.

Platform governments

Governments operate highly efficient and effective online platforms that facilitate economic exchange and most other activities.

Most governments belong to political blocs with platforms that interact with each other but not with other blocs.

Infrastructure is of paramount concern in the national development and security strategies of countries.

Large amounts of data in government control come with great responsibility, and the need for checks and balances.

Corporate connectors

A small number of global technology companies function as one-stop shops for every aspect of life.

Through their economic power and analysis of popular will, technology corporations have gained legitimacy to take up space in global governance.

Many fields previously under the charge of governments are now in the hands of corporations.

Trust in corporations is high and the main allegiance of most people is to a firm, not a government.

#Me2.0

Summary

It is 2035, and people around the world have harnessed digital technologies to create new social movements and community structures to advance their needs. In so doing they have challenged the dominance of territorial governments and private sector firms, creating a revitalised third pillar within the global economy, society and governance system: the civil sector. People use their online identities in increasingly active ways to further their economic opportunities, civic participation and personal development, both in digital and physical space. Technologically enabled peer-to-peer-like organisation structures, grass-roots initiatives and self-organised global, regional and local communities have empowered citizens like never before.

#Me2.0

- People have harnessed digital technologies to create new regional and global communities to better advance their interests.
- These movements have challenged the dominance of governments and firms, creating a powerful third pillar of the global system: the civil sector.
- Communities use technologies effectively to tackle local and global challenges.
- Polarisation between groups and questions of accountability remain challenging.

Together with more readily available technologies, value shifts have driven people to mobilise around common goals on both an ad-hoc and ongoing basis. As environmental degradation and resulting inequalities increased, trust in global institutions to develop tangible solutions and protect common resources fell significantly. Citizens began to take the initiative to come together and look for new ways to build low-impact lifestyles, foster better health outcomes and recreate a sense of community. Small-scale experiments and pilot initiatives on a local level, and collaboration through connected digital communities on a global level, allowed them to forge a new way path. These new communities no longer fit with previously established definitions and boundaries of civil society organisations, with many adopting new formats and approaches. Some blend online and offline activities and have evolved from existing structures to support particular interests; others emerge ad hoc based on a spontaneous expression of a grievance, trending hashtag or current event. Communities at the global, regional and local levels connect, co-ordinate and compete in a complex cross-cutting pattern of interactions.

Rather than displace governments and business entirely, however, these new movements and organisations serve as a complement and counterbalance, providing the necessary political pressure and practical examples to force governments and firms to perform better in meeting citizen and consumer needs. Nevertheless, new challenges have arisen with the growing power of these societal movements and organisations, including diverging outcomes and polarised views among members of different communities, and inconsistent standards of transparency, accountability and democratic decision making.

Signals: Self-organised communities, digital commons and open source intelligence

Strategic foresight uses signals of change observed in the present to point to plausible new trends or discontinuities that could emerge and grow, and result in a future scenario which differs from current expectations. The following signs of change are already visible and, if they continue to grow, could give rise to the scenario in the previous section.

The Internet has brought about a range of self-organised communities and online mass collaboration projects. Examples include wikis (most famously Wikipedia), open licensing organisations, open source software repositories and communities, and peer-to-peer support networks. The architecture of the Internet itself was developed partly through a community approach by a group of computer scientists, engineers and technicians.

Online community organisation led to powerful action taken offline, most famously during the Arab spring or the 2009 Iran "Twitter revolutions", but also in the context of the "Fridays for Future" movement, which pushed for greater action to tackle the environmental crisis, or the "#MeToo" campaign, which called for action against sexual harassment. Often these networks serve to fill a gap in management or legislation, which is not adequately addressed by governments or corporations. For example, mutual-aid accountability is an effective response to online harassment on platforms such as Twitter, and mutual-aid mentorship technology can help track spam responders, for example on Wikipedia (Matias, 2015).

The Internet has allowed people to protect and manage common resources in new powerful, community-driven ways (Hesse, 2008; Walljasper, 2011). For example, the citizens of Sarantaporo, a small village in Greece, founded an initiative to deploy local broadband infrastructure as a commons in the absence of dedicated efforts by telecommunication networks or the government (Mölleryd, 2015). Other people have formed their own commons to mix music and videos, as have scientists who use open access, community-managed journals to publish their research as an alternative to commercial publishers. Among many others, digital commons are also devoted to sharing university course curricula and to gathering together neuroscientific research found across the web (e.g. Open Course Ware by the Massachusetts Institute of Technology).

Similarly, people are taking steps to exercise control over artificial intelligence (AI), machine learning methods and the ways in which data are processed and used. Open source intelligence (OSINT), which allows actionable and predictive intelligence to be obtained from public, unclassified sources, is also gaining traction. Open source AI technologies and AI kits, based on open source platforms, are making machine learning projects accessible for everyone. In addition, individuals increasingly want to understand the algorithms behind the appliances they use. For example, AutoPilot, an autonomous car development platform, is working on a software that could allow its users to see the visual elements the AI is tracking when driving (Nvidia, 2020).

How this world came about

In 2019, the Internet held unprecedented opportunities for community-based collaboration and empowerment. Increasing availability of assets such as open source software, broad information sources and large-scale databases have given individuals the means to be creative, experimental and effective in powerful ways. With digital literacy and related skills improving on a global scale, coding and software development have shifted from an expert field to the mainstream, with most digital appliances becoming accessible for everyone. More and more individuals have discovered how technologies such as AI, 3D printing and distributed ledgers could allow them to make real-life improvements in their own communities.

A spate of data leaks and publicity surrounding large-scale, data-driven manipulation, as well as environmental and ethical scandals in the corporate technology sector, led to a growing sense of disempowerment among individuals online. As a response, civil society groups began to advocate for more transparent data management policies, users started to boycott certain providers, and community-driven alternative services and platforms started to emerge, challenging the dominance of corporate ones. As a means to regain trust, both governments and corporations sought community advice, and consulted with civil society to design more legitimate and safe digital products and services.

Meanwhile, deep uncertainty and volatility linked to climate crises and inequality resulted in social unrest, disrupting "business-as-usual" local and national political systems. Few systemic changes were implemented on time, and in most parts of the world, pollution, waste and emissions kept increasing while climate disasters hit vulnerable communities particularly hard. Citizens looked for ways to fill the solidarity gap left by corporations and government, and built up trust in local initiatives, communities and constituencies. As a result, the civic sector expanded significantly, equipped with digital technologies that enabled these groups to adopt their own governance rules, develop effective decision-making mechanisms, and create value locally and sustainably. Examples include the creation of AI and blockchain-enabled experiments, for example, to grow crops, introduce safe lending systems and build sustainable, community-based housing models.

What this world looks like

Under the **#Me2.0 scenario**, Latvia's civil sector functions as a central new pillar addressing national and local issues that were formerly within the government's purview. Society harnessed the untapped potential of Latvia's digital infrastructure and created local and cross-border groups of like-minded individuals to address issues in a direct, tailor-made manner. This might include co-ordinated actions for environmental protection, and the gathering and sharing of information both online and in person through widespread automation and use of open source AI (e.g. for transport and logistics). As a consequence, Latvians generally have high confidence in the potential of their individual actions to effect change, as well as the potential of concerted efforts. In communities with high digital literacy, online education opportunities are widely used, enabling citizens to specialise in a broad range of professional fields and to access international job markets.

However, due to a sharp generational and rural-urban digital divide which excluded some communities from digital emancipation processes, society might have become increasingly polarised. This could include a growing division between citizens living in the same geographic areas whose membership of digital communities and cross-cutting social movement increasingly shapes their identity and their lives. Those who turned away from the digital sphere due to a lack of skills, or increased difficulty with distinguishing between fake news and legitimate information, were left behind and find participating in public discourse difficult. Populations living in less vocal or well-organised local or online communities have a lower capacity to lobby for government services and economic activities, and find themselves increasingly vulnerable to digitally organised criminal activity.

Insights about Latvia's digital strategy

The #Me2.0 scenario highlights the potential importance of emerging new actors in the civil sector and the associated implications for Latvia. It underscores the potential benefits of tapping into specific, tailored knowledge of communities and social movements of various forms – online and offline, local and internationally connected, formally organised and ad hoc. Such communities may function as a powerful means to generate feedback about the varying needs of Latvians for digital learning or public services based on their differing regions, age groups or ethnic background. Minority-oriented social movements could also take on an important role in fostering social cohesion within Latvian society by generating data and insights to improve inclusion and diversity policies.

The scenario points to opportunities that could arise from promoting digital community building in an inclusive and ethical way, in order to empower citizens and mobilise ideas, talent and energy towards achieving societal goals. Conversely, the growing importance of digital communities might also heighten the risks posed by increasing divisions and disputes over values between members of different groups. Online division and polarisation could create closed communication circles with each promoting its own relative truth. Furthermore, risks associated with enhanced opportunities for organised criminal activity quickly become apparent. Digital communities based in Latvia may be well connected to foreign partners, undermining established national security and ethical standards. Overall, the scenario poses the question of which new collaborative structures and frameworks would best allow the country to connect new actors with established ones to create economic and social innovation, while simultaneously keeping citizens and communities safe.

Based on the #Me2.0 scenario, policy makers in the digital field could explore a range of strategic questions:

1. What role should communities, local initiatives, peer-to-peer approaches and **decentralised technology development** play?
2. What new **resources and support could be made available to civil society organisations** to help them connect digitally on a global scale?
3. How can **digital community building be promoted**, for example through local initiatives that are co-ordinated and promoted online, such as participatory municipal budgets?
4. How could **emerging technological values disputes be identified** and foster honest and factual debate?

Platform governments

Summary

The year is 2035 and platform governments have played a decisive role in shaping the digital transformation in two main ways. First, most governments now provide and leverage a main platform for digital activity in the economy and society. Second, many governments have become integrated into digital megaregions, openly sharing data internally while maintaining digital borders with the outside.

Platform governments

- Governments operate highly efficient and effective online platforms that facilitate economic exchange and most other activities.
- Most governments belong to political blocs with platforms that interact with each other but not with other blocs.
- Infrastructure is of paramount concern in national development and security strategies.
- Large amounts of data under government control carry great responsibility, and necessitate checks and balances.

In this world, government platforms channel digital activity by citizens, corporations and societal organisations, a process which allows for the collection and analysis of large amounts of data by the state. These detailed insights allow governments to provide highly efficient service delivery and develop policies in a highly targeted manner. Platform users have a crypto-verified digital identity that ensures trust as well as a seamless transition between the analogue and digital world.

Most platform governments are members of a bloc or alliance, operating as part of a common digital megaregion. Each region interconnects societies closely on the inside and separates them from the outside through a digital border. Data flows freely between all members of each region, and governments are able to use aggregated data analysis to make informed policies. What used to be the World Wide Web has diverged into multiple national and supranational systems on the one hand, and ungoverned digital spaces outside any institutional control on the other. Data, trade and investment flows between regions are highly limited and undergo thorough scrutiny.

Signals: Digital public services, citizen ranking, unique identity systems, foreign investment screening and provider regulation

Strategic foresight uses signals of change observed in the present to point to plausible new trends or discontinuities that could emerge and grow, and result in a future scenario which differs from current expectations. The following signs of change are already visible and, if they continue to grow, could give rise to the scenario in the previous section.

A range of signals in the present show how governments are taking a more digitally driven approach to interacting with citizens – expanding digital service delivery, providing citizens with unique digital identities and using big data for rating purposes. Furthermore, a number of governments have taken steps to ensure control over various layers of their digital space through measures such as foreign investment screening, data localisation and provider bans.

A wide range of countries have established various forms of digital service delivery. The Estonian government was an early adopter in this regard, creating e-Estonia, a countrywide digital initiative using electronic solutions to facilitate citizen interactions with the state. Numerous online services such as digital identification, digital signatures and online medical prescription have been made available to citizens, initiatives similar to which exist in New Zealand, Singapore and the United Kingdom. The backbone of e-Estonia is an underlying data exchange platform called X-Road that links all information systems of the government to make data easily accessible. The system was designed to scale as new e-services and new platforms come online and other governments join the network. Governments also

seem to have the lead in the field of digital currency; for example, the European Union is debating the introduction of its own cryptocurrency (Guarascio, 2019).

Government identification systems are evolving in many parts of the world, often as an essential component of digital government. India has set up the world's largest biometric system, Aadhaar, with more than 1.2 billion registered citizens. The Unique Identification Authority of India (UIDAI)[1] issues a 12-digit number to residents which allows for greater transparency of identities and the roll-out of government welfare schemes and programmes. Aadhaar is a key component of Digital India and was designed as a strategic policy tool to improve social inclusion and public sector delivery as well as budget management. Other national electronic identity programmes have been launched in Algeria, Cameroon, Italy, Jordan, Senegal and Thailand.

Governments use digital means and big data to create personal profiles and rate or predict behaviour. The People's Republic of China (hereafter "China") is pioneering a nationwide "social credit" system, which uses big data to assign a score to natural persons and legal entities, drawing on a wide variety of sources. The system centralises data under a single identity, assigns a score, and adjusts interactions and governmental services accordingly. It is envisioned as a powerful tool for the enforcement of laws, regulations or other party-state targets (Shi-Kupfer and Ohlberg, 2019). Other countries are working with similar rating mechanisms in specific areas. For instance, Canada's new Express Entry system for the selection of labour migrants allocates points for a broad variety of socio-demographic characteristics to predict successful labour market integration. In the United States, social media information is required for visa applicants, in order to create risk profiles.

Many countries have increased scrutiny over foreign investment, a move that may allow them to protect their own digital markets. In 2017, China introduced the Cyber Security Law, which defines key categories such as "critical infrastructure" and "personal data" in a broad way, presumably as a means to exert control over foreign investment. The Cyberspace Administration of China is authorised to pursue a cyber security review of all products and services used in critical infrastructures – including the exposure of source codes (KPGM, 2017). Some governments such as Germany have adopted a more explicit approach in recognising digital issues in national security, while others such as the United States are thoroughly scrutinising foreign investment in digital businesses.

Other ways in which governments exert influence over the digital space include data localisation rules, restrictions on cross-border data flows and Internet provider bans. Legislation of cross-border data flows can take various forms. Some require *ex post* accountability for the data exporter if the personal data sent abroad are misused, others make data transfer subject to various types of safeguards and some are subject to case-by-case authorisation (Casalini and López González, 2019). Data localisation requirements stipulate that firms must store certain digital data in host countries and thus set up storage infrastructure. Both requirements are becoming more common and tend to target particular types of data, in particular those with a personal or sensitive component. Examples of provider bans include the introduction of the Russian Sovereign Internet Law to replace the Domain Name System, and bans of certain Internet services by governments as a means to support the establishment of local providers (BBC News, 2019).

How this world came about

Between 2019 and 2035, a few governments employed a more active approach to digital transformation, introducing digital platforms to improve their way of working. At first, citizens and corporations used the platform for a limited number of services, such as managing health records, filing taxes and registering a product or business. As satisfaction grew with the convenience of this approach, services expanded gradually into fields such as financial accounting, smart contracts and skill development. No major hack or other breach that would have impeded trust occurred during this phase. Instead, trust in the system and among its users was high and the use of unique digital identities improved online accountability and traceability. As the number of interactions through the platform increased, its usefulness grew and its name began to be synonymous with the Internet.

Thanks to the increasing amount of data collected and the interlinking of databases, governments gained unprecedented insights into the behaviour, needs and preferences of their citizens and companies. Policy making became more targeted and data-driven, serving the needs of individuals and

organisations in fast, customised and adaptable ways. For example, the medical records of a child born in a hospital would automatically be analysed by artificial intelligence, and used to allocate government financial support and identify schooling options years ahead of time. Despite existing privacy concerns, the majority of the population voiced high levels of satisfaction with the new system. Political support rose for the implementing platforms, with better social and economic outcomes reported than for their less digitally driven neighbours.

Acceding to pressure from pioneering governments and public demand, other governments followed this example and started building their own platforms, or commissioning existing ones to adopt new approaches. Within a few years, a highly governmentally driven approach to digital transformation became the dominant model with platforms consolidating further to benefit from economies of scale. Only a few countries opted out of this trend by taking a more passive approach, or alternatively using government power primarily as an instrument to slow down the digital transformation and its impacts.

Countries connected to each other within digital megaregions eventually restricted data flows from and to other regions in order to protect local providers and exert better control over data management. Security concerns gave rise to restrictions on foreign investment in the digital space and eventually ensured that rival regions did not possess a financial or political stake in the platform. This allowed for effective protection of citizens' personal privacy and industry intelligence vis-à-vis external threats, and necessitated strong digital borders consisting of firewalls and cyber protection.

However, these measures were partially offset by the additional opportunities this approach created for local digital companies. Some smaller countries created an alliance permitting mutual free data flows based on common privacy standards and a shared data frontier with the rest of the world. A few global institutions emerged to enable trusted data flows between different countries or blocs, respecting their various conditions.

What this world looks like

Under the **Platform Governments scenario** Latvia becomes a digital platform government, within a bloc of like-minded states. Building on its high system integration capacity Latvia develops a sophisticated data collection and management system and fosters the continuous adoption of services by the government platform. This enables citizens, businesses and civil society actors to access high-quality services more easily, with a concomitant rise in overall trust in government. As with all governments, however, institutional mechanisms and incentive structures do not always allow Latvia to make the most of new data insights, and as a result some opportunities are missed resulting in sub-optimal outcomes.

Latvia co-ordinates closely with other countries in the same digital bloc, which may be limited to Baltic or Nordic countries, span Europe or include like-minded partner countries geographically dispersed around the world. While intra-state and intra-bloc data circulation is generally welcomed as a means to improve quality of services, data leaks to agents outside Latvia's digital region are feared. Indeed, as a result of a prior lack of investment in a comprehensive cyber security framework, Latvia has faced various large-scale hacks and cyber-attacks. Consequently, there is heightened sensitivity around international trade (especially between blocs), which is increasingly associated with national security concerns. Other platform governments under the control of authoritarian leadership have made use of their administrative capacity to exert excessive data-driven influence over their citizens' lives. This has led to heightened awareness in Latvia, where initial steps are taken to mitigate the susceptibility of the system to any kind of abuse.

Insights about Latvia's digital strategy

The Platform Governments scenario highlights challenges and opportunities related to the development of an integrated digital information management system for government, with necessary safeguards both within the Latvian government and internationally. It raises the question of the role the Latvian government wants to play in the digital economy and society, and the choice of digital partners with which it should tighten connections. The scenario highlights the long-term implications of digital partnerships with other countries and the need for common value sets and democratic beliefs.

Conversely, a weak government information management system could elevate the risk of Latvia falling behind countries willing to take bolder measures. Investing in a more capable and integrated approach could allow Latvia to tailor and adapt policies according to its population's needs, better achieve economic innovation and citizen well-being, and strengthen the ties of Latvians with their country. For example, such a system could provide the Latvian government with detailed real-time knowledge about the capabilities, health, well-being, attitudes and behaviour of Latvian citizens and firms, allowing the government to create new and adaptive employment opportunities, foster and monitor skills uptake and react to the concerns of Latvians more strategically.

The scenario also underscores a number of significant risks linked to abuse of an integrated system. If a government with extremist tendencies or groups with criminal intent were to access the keys to a highly detailed and effective information management system, they could potentially abuse it in numerous ways. This could include targeting political opponents, advancing private economic interests or manipulating the beliefs and behaviour of citizens through targeted political advertising. As the scenario demonstrates, whichever government entity were to carry out extensive data gathering and analysis of citizens, would effectively control a substantial digital intelligence capability. Overall, Latvia must consider carefully the choice of data-driven capabilities it wants to build up, and evaluate how it can establish a leadership approach and the necessary systemic checks and balances, to ensure data insights are used for beneficial decision making for all.

Based on the Platform Governments scenario, policy makers in the digital field may wish to explore a range of strategic questions:

1. What checks and balances are built into current digital policies, and would they be sufficient to ensure trust, security and accountability if the state digital infrastructure were to grow considerably in scale?
2. Does a **country's geopolitical place in the world** present new challenges from a digital perspective and what decisions could be taken today to avert potential dilemmas?
3. Can **greater state involvement in the digital economy and freer markets** be reconciled, in order to deliver greater well-being for citizens?
4. What **kind of digital government** does our country want?

Corporate connectors

Summary

In this world of 2035, a small number of global technology companies function as one-stop shops for every aspect of life, from socialising to health monitoring, learning and consuming. Through their economic power and constant analysis of popular will, they have taken a more active role in global governance. Many public sector activities in fields such as infrastructure deployment, school curricula and security provision have been outsourced to these private companies.

Corporate connectors

- A small number of global technology companies function as one-stop shops for every aspect of life, from socialising to health monitoring, education and security.
- Trust in corporations is high and the main allegiance of most people is to a firm, not a government.
- Through their economic power and constant analysis of popular will, technology corporations have gained legitimacy to take a more active role in global governance.
- Many fields previously under the charge of governments, such as public infrastructure provision, school curricula or monetary policy, are now in the hands of corporations.

Individuals, referred to as citizen-consumers, have developed strong connections with large digital corporations, and the main allegiance of most people is to a firm, not a government. Government tax revenues have dwindled, and the number of public officials has more than halved over time. The general response has been to integrate private sector actors further in a range of policy fora. Lobbyists of technology companies stand openly as candidates in local and federal elections, and the United Nations General Assembly now includes delegations of major corporations.

Signals: Superstar firms, market concentration and fields of public interest

Strategic foresight uses signals of change observed in the present to point to plausible new trends or discontinuities that could emerge and grow, and result in a future scenario which differs from current expectations. The following signs of change are already visible and, if they continue to grow, could give rise to the scenario in the previous section.

Many firms today are significantly larger than the most productive firms decades ago, with a significant increase in industry concentration recorded in Europe and North America (Bajgar et al., 2019). Some globally operating "superstar" firms have a larger revenue than entire states and vast user bases, lending their actions and decisions a new global scale and significance. These winner-takes-most dynamics have increased the economic and political power of a handful of firms, particularly in the high-tech sector.

Network externalities and the scale of consumer and industry data has led to concentration among several markets. Corporations operating digital platforms collect granular user data on an aggregate level that allows them to build predictive models capable of determining consumer preferences and anticipating behaviour (OECD, 2018). Customer-centred business intelligence has not only evolved as a new mechanism for corporations to gain economic power, but has also given corporations insights into human preferences on an unprecedented scale.

Some of these powerful firms have begun to play a role in determining the priorities of policy institutions, for example in the field of migration. The technology sector relies strongly on migration to fulfil their skill needs. For instance, in Silicon Valley close to 60% of workers in STEM jobs with a bachelor's degree or higher are foreign born. Among software engineers, the share rises to 70% (Kerr et al., 2016). The ability to easily bring in foreign workers is an important factor for firms when selecting hub locations, with Canadian and American cities competing in the recent Amazon HQ2 tender process on the basis of ease of bringing foreign workers.

Furthermore, technology firms exert increasing influence over issues of public interest, for example in the education, health and housing sectors. Today, many schools and universities rely on cloud services proposed by Google or Microsoft. The former has developed a specific product, Google Classroom, which enables students and professors to exchange among virtually, as if in an actual classroom. In terms of health care, Alphabet, the parent company of Google, has invested significantly in the use of technology to better understand health, and also employs data generation, detection and positive lifestyle modifications to tackle disease, for example through the acquisition of Fitbit (CB Insights, 2019). Regarding smart city planning, large-scale corporate projects are on the rise. However, the remodelling of the Toronto waterfront into a "smart city" by a US company, with features like snow-melting roadways, an underground delivery system and a range of data-collecting sensors, has raised privacy concerns (Deschamps, 2019).

How this world came about

During the initial phase of consolidation, leading up to 2019, a race between technology corporations for market share among citizen-consumers and suppliers ensured a fair degree of competition. This kept prices low or even free for citizen-consumers and fees low for suppliers. However, as membership solidified and no new competitors emerged, all platforms began simultaneously to raise their prices and fees. There was no proof of collusion and unfounded allegations were quickly removed from social media sites. Some suspected that what might resemble co-ordinated action by platforms may simply be a product of rational optimisation advised by their respective business intelligence AIs. Productivity growth, while extremely high initially, started to slow, in part as a result of new innovators being acquired and subsumed by the platforms rather than being able to grow to scale.

The increasing influence of corporate connectors was accompanied by new responsibilities, but also with increasing capacity to make decisions on issues of public interest. For example, the challenges of social media echo chambers, censorship and free speech, and fake news were largely addressed by the platforms, with governments lacking the knowledge and means to remain involved. This trend led to the emergence of several online deliberation spaces which started to influence digital decision making. This new form of democracy, characterised by constant nuanced online engagement, enabled corporations to understand the evolving preferences of citizens better than ever before. However, the inability of platforms to get every decision right ensured that national democracy continued to represent local interests. Governments appointed tech ambassadors to lobby and represent the interests of their residents vis-à-vis corporations.

Digital corporations continued to pay very little corporation tax. Due to a lack of financial means, governments started outsourcing many of their functions to the corporate sector. Many quality-control regulations, for example on taxis and hotels, were replaced by rating systems based on sensors and checks imposed by the platforms that connect them with customers. Over the years, corporate connectors became involved in an increasing number of policy fields ranging from infrastructure to education, health and security. Due to the high quality of the services they provided, most citizen-consumers continued to be loyal and trusted them with data-driven insights into their daily decisions. Nonetheless, movements critical of increasing corporate influence persisted, but struggled to gain traction and reach a large audience as their messages frequently disappeared from social media channels.

By 2030, the idea of citizenship had taken on many new and different meanings. In addition to statehood, individuals developed increasingly close connections with large digital firms or online platforms that provide an extensive range of services and support in exchange for loyalty, personal data and fees for premium features. Eventually, this new form of digital citizenship became transnational, just like the firms that offer it.

What this world looks like

Under the **Corporate Connectors scenario**, Latvia's economy has become closely intertwined with large global corporations, driving a number of national, regional and local companies out of business. Many Latvian SMEs prospered initially by integrating into a corporate ecosystem in order to access new global markets, but now find their profits squeezed as the intermediary takes a larger share. While convenience for citizen-consumers rose due to a streamlined interface and internally co-ordinated services, this has required and resulted in substantive amounts of sensitive personal data being collected and controlled by corporations. These firms have leveraged their technological supremacy to offer much stronger cyber security for such data, rigorously safeguarding them from potential hacks or leaks. However, access to this information by governments or others for public benefit is highly limited. As a result, Latvia's government is subject to significant corporate influence, relegating it to a bystander position, and policy oversight has become much harder.

Global corporations have seized the opportunity resulting from government services increasingly lacking in precision and quality to replace them with their own, more tailored and convenient offers. As a result, many services previously provided by government such as infrastructure, health care or education are now at least partly in the hands of corporations. Due to the often high levels of citizen-consumer satisfaction, trust in corporations is high overall, but the needs of vulnerable and economically disadvantaged groups are often neglected. Latvia consequently faces a high level of inequality that the weakened government struggles to tackle effectively.

Insights about Latvia's digital strategy

The Corporate Connectors scenario highlights challenges and opportunities related to a growing presence of large global technology firms based outside the country, their deepening influence over Latvian citizens, businesses, public policy and society, and their further involvement in fields of public interest in Latvia. Potential risk associated with this scenario could heighten if Latvia were to become dependent on one or a small number of technology providers. Not only could such arrangements lock Latvians into certain technologies, it could also weaken Latvia's negotiating position when adapting systems at a later stage. In addition, close ties with a particular provider could affect the Latvian government's leverage concerning regulation and enforcement issues, both nationally and in a multilateral context.

More broadly speaking, the scenario underlines the need to identify policy levers nationally and multilaterally to ensure the potential influence of corporations over Latvia's economy and society is kept in check. This could require reinforced strategic international partnerships in fields such as competition and data policy, but also demand a systematic screening effort in national policy making. For example, it is possible to envisage a situation where all Latvian schools that use applications from a particular technology provider creating incentives to adopt the same ecosystem in other personal and professional contexts or even for administrative matters. Ultimately, this could create a path dependency making changes to Latvia's broader technology procurement strategy increasingly costly. Decisions in strategic fields such as education and data management could end up in the hands of a private corporation where profit-driven incentives may matter more than serving the needs of all citizens equally.

Conversely, Latvia may enjoy various benefits from collaborating with globally leading technology providers. Such agreements could allow the country to achieve faster roll-out of new technologies and services, simplify procurement systems within an established partnership and benefit from economies of scale when working with the same provider in various contexts. The scenario raises the question of which measures best ensure that democratically chosen objectives are respected and advanced within any private-public partnership. Overall, it amplifies the need to limit the influence that private actors can acquire over fields of public interest and determine the types of regulation that best ensure the protection of Latvian citizens and their diverse needs and interests.

Based on the Corporate Connectors scenario, policy makers in the digital field may wish to explore a range of strategic questions:

1. What **strategic partnerships and collective initiatives** would enable Latvia to exert maximum leverage in favour of public well-being in a world where firms outweigh states?
2. How can **competition between digital services** be promoted in order to make it easier for consumers to switch providers?
3. Should Latvia encourage or participate in initiatives to **rate and rank firms by quality of cyber-security**, and require such information to be provided as a "digital product label" to inform consumer choices?
4. **What kind of access** does Latvia want to give private corporations in **which policy fields**?

Strategic perspectives for Latvia to consider

The foresight process draws on the higher-level implications of Latvia's potential actions in each of the scenarios: How well would any option perform under various future contexts and can any "no regrets" option be identified? Which current beliefs and expectations built into policy making may be challenged by future disruptions?

The outlined options offer a complementary input to the specific and technical recommendations outlined in the following chapters of this report. They are meant to enrich Latvia's digital strategy with long-term, strategic thinking offering an additional lens to aid the prioritisation and selection of actions. Each of the actions identified may provide an opportunity to move closer to one of the desired future directions identified above (see section "Directions for a desirable digital Latvia"), while simultaneously strengthening Latvia's capacity to deal with potential future changes. Each of the following paragraphs will describe high-level implications for Latvia and list exemplary strategic options the government could consider in this context.

Latvia is a country with numerous strengths that can allow it to thrive in a digital future, but also faces certain challenges:

- Latvia's internal connections provide the ability to collaborate effectively across various policy and industry fields. Collaborations between policy makers and the research and academic field have potential for further development, particularly given the high quality of Latvian education.

- Latvia has various structures in place that allow for direct feedback loops between the government and the public. These channels have the capacity to generate valuable inputs for policy makers, but also pose challenges related to transforming these insights into evidence-based policy making and strengthening data-driven decision making.
- Latvians are keen to take up digital technologies and share high ambitions for their government overall, generally trusting in its ability to deliver on a digital strategy. At the same time, there may be room to share more responsibilities with other stakeholders within the country, for example by creating new enabling factors for the private sector or taking better advantage of those already present.
- Stakeholders have identified a risk that hasty regulation in the digital field may hamper innovation opportunities.
- Latvia has great potential to be an agile, adaptive and fast-moving country as a result of its well-connected, relatively small population. However, the country has limited opportunities to lead on international issues such as regulation of global corporations and must be able to respond strategically to changes outside its direct control.

Strengthen Latvia's internal and external partnerships for digital transformation

The scenario discussion in the previous section provided various concrete future contexts in which success depends on a whole-of-society approach to digital transformation in Latvia. This would require strengthening co-operation and effective collaboration across government, business and civil society organisations to advance key digital priorities. Such partnerships are necessary not only to leverage the data, insight and expertise held by different partners, but also to ensure an ongoing healthy diversity of power centres and checks and balances within Latvian society. In addition, the scenario discussion pointed to the strategic importance of networks and partnerships extending beyond Latvia's borders. Strengthening these partnerships will allow the government to leverage necessary regulation in fields where Latvia alone can only exert limited influence, such as data governance and competition policy. Partnerships can also help to keep the Latvian digital ecosystem (e.g. information management systems) connected and compatible with like-minded partners sharing a similar set of values.

Strategic data partnerships. The scenario discussion also emphasised the value of large-scale data analytics for making accurate, evidence-based decisions in various fields. All three scenarios highlight the political and economic influence that comes with access to insightful digital data (whether by communities, corporations or governments). For Latvia, this underscores the need to respect appropriate limits and safeguards in cases where various actors obtain access to sizeable data sets providing granular and insightful information on any given issue, according to the level of data sensitivity potential. This could include limiting the number of agencies with access to specific kinds of data. One particular perspective for action here is collaboration between academia and industry.

Accordingly, data partnerships are of crucial importance for stakeholders in the academic, business and development field. In order to reap the benefits of big data analytics, Latvian stakeholders must establish strategic systems that allow for compatible, value-based data collection, sharing and analysis. Options for action may include:

- co-operating with leading academic institutions abroad and other parties to collect a critical mass of data and improve data co-ordination
- ensuring compatibility between networks and data providers
- creating a platform for integrating and sharing government data with third parties such as civil society and corporations in a controlled and ethical way – taking into consideration, in particular, the value as well as the sensitivity of health data
- continuously strengthening a digital security and ethics checklist system for any government decision, for example in the field of public procurement
- formalising a strategy of collaboration between digital platforms of other countries in northern Europe
- establishing multi-stakeholder (involving academia, private sector, technological community, civil society, government) consultation procedures on the creation of regulations in order to avoid excessively rigid regulations.

Industry-university partnerships. There is potential for mutual benefit between higher education institutions and industry arising from developing and sharing digital knowledge and skills in innovative and impactful ways for Latvia's economy and society.

Ministry-university partnerships. Universities are a key potential partner in digital transformation, bringing a necessary complement of independence, objectivity, accountability, in-depth analysis and evidence to inform policy making, decision making and implementation on digital policy issues. Such partnerships can help establish necessary checks and balances to allow Latvia to plan for futures characterised by enhanced data-driven control by governmental or private sector actors, among others. The following actions could help develop and reinforce effective partnerships between universities and government:

- taking advantage of existing flexibility in policies such as procurement and other funding mechanisms to enable longer-term collaborations, so that partners in government, universities and institutes can invest in developing the necessary expertise and relationships – and identifying and addressing potential barriers
- encouraging universities to support policy making, for example through analysis of policy implementation
- facilitating staff rotation and exchange between universities, business and government, to help address gaps in expertise and longer-term perspectives in public service.

Language technologies. Recent successes with developing language tools, such as machine translation and the technologies that support them, could hold potential for Latvia to further specialise in a field with multiple future opportunities in the civic, public and private sectors.

Rail Baltica project partnerships. The Rail Baltica project is a major cross-border partnership offering digital opportunities for Latvia, among others. Given the project's innovative nature and technology-driven planning (e.g. regarding the cloud-based Common Data Environment), Rail Baltica offers opportunities to strengthen ties with neighbours on digital matters and further integrate Latvia's digital ecosystem. The project can also serve as a stress-test for Latvia's capacity to engage with various stakeholders, ensure digital safeguards and streamline public-private partnerships. Potential avenues for further development include:

- engaging with communities on opportunities offered by the opening of a new high-tech high-speed railway station
- reviewing in advance opportunities and risks related to opening up the technology and offering procurement contracts to private firms.

Project funding alliances. Government needs to lead and further co-ordinate and consolidate the funding efforts of firms, communities and academia in fields such as large-scale digital infrastructure (e.g. transportation or 5G projects) and ICT research and development. This would enable better alignment of expectations and the creation of synergies among different stakeholders and strengthen their position when negotiating with international partners. Actions to consider include:

- partnering with digital finance and Fintech experts to set up open source co-ordination systems aligning funding partners on the basis of shared objectives and key performance indicators, and providing access to civil society and community partners
- connecting funding alliances to international partners, for example at the EU level
- using alliances to foster knowledge exchange between private sector, civil society and academic actors.

Identify smart approaches to education and skills for adaptive, critical Latvians

A digitally empowered public can serve as an important source of digital innovation, entrepreneurship and productivity. A digitally capable citizenry can also help hold governments, corporations and other organisations to account for their digital policy choices, and enable society to navigate the many challenging trade-offs related to digital transformation, such as the automation of work and the collection and use of personal data. In addition, the strategic foresight process highlighted the point that in a digital, complex and fast-changing world, there is an increasing need not only for "digital skills" such as data visualisation or manipulating AI, but also skills like creativity, problem-solving, adaptability and critical thinking.

Applied learning programmes for students. To be prepared for a complex and fast-changing digital world, young Latvians must not only acquire theoretical ICT skills, but also learn in practical ways about the benefits and – just as importantly – any potential dangers that digital transformation can engender. From this perspective, practical collaborations between the formal education sector and firms, research institutions and communities based in Latvia could be beneficial, and could take various forms, for example:

- establishing long-term partnerships between Latvian schools and companies to offer practical learning opportunities and strengthen ties between Latvian talent and local employers
- offering case-study programmes, innovation labs or hackathons in schools in collaboration with Latvian private sector partners, thereby allowing students to tackle real challenges facing Latvian companies and apply their theoretical knowledge in a practical manner, thus preparing the next generation for potential future challenges of the digital transformation, fostering their innovation capacity and strengthening the links of Latvian companies with young talent to ensure local SMEs and established companies have access to suitable staff in a context of fierce international competition
- making use of these partnerships to ensure a faster feedback loop between practitioners and educators in order to adapt Latvians' skills and school curricula continually in accordance with future needs, and better leveraging existing capacity within firms through connections with academic or community partners.

Human capital investments. Human capital is a well-known driver of economic growth and innovation, and the information-driven digital economy has further accentuated this dynamic. In order to harness the potential of an economy heavily reliant on human resources, Latvia must ensure continued flows of investment into its biggest asset – its employees. To support continuous learning even after the end of formal education, Latvia could explores ways to incentivise firms to invest in their employees. These could include:

- rolling out (further) programmes for employer-sponsored continuous vocational training (i.e. provided or paid for at least in part by firms)
- introducing new incentives and funding (i.e. firm-level incentives) for specific company-led learning and training programmes in the ICT field
- systematically assessing the policy environment for Latvians working in the gig economy, including potentially an assessment of the adequacy of Latvian labour policies, insurance schemes and work contract formats for gig economy workers.

Digital learning hubs. The scenario discussion – especially the #Me2.0 scenario – highlighted the potential of community-driven digital innovation. Granting Latvians across the country better access to open source tools and learning opportunities to become digitally savvy would give them a greater stake in the country's digital development. In this context, the workshop pointed to the option to further develop Latvian digital learning hubs that connect with existing infrastructure such as regional libraries and education institutions – potentially building on the success of the DigiHubs network.[2] This would enable training opportunities to be offered across Latvia in urban and rural areas alike, and could serve as an accelerator for digital transformation. It would also enhance digital skills among all age groups and respond better to diverse needs across the country. E-learning platforms (including technical infrastructure and learning content) should be developed, in order to increase opportunities for distance learning and e-learning.

Identify pathways to an inclusive digital Latvia for and by the people

The scenarios highlight both sides of digital transformation – the opportunities technology creates for people to voice their opinion and become active, as well as the potential threats of technology to equality, inclusion and individual control over their data and lives. Deliberate efforts can help to maintain citizen trust and provide Latvians with new means to voice their needs and opinions and fulfil their own digital aspirations. These efforts can leverage economic and social innovation stemming from all regions, sectors and institutions of Latvia.

Social impact funding and crowdfunding. Potential opportunities to foster inclusive economic development can be envisaged in a few ways:

- providing open source tools to help funders track their progress towards achieving key social performance indicators
- helping citizens, communities and businesses track the progress of funded projects and contribute to achieving them
- developing new crowdfunding tools in collaboration with community leaders, for example through reward systems or gaming approaches.

Secondary data use legislation. Further attention may be need to be paid to the secondary use of data and anonymity, particularly in relation to the sale of medical data to third parties and countries. Potential measures include:

- defining private data as a good with quantifiable economic value that takes into account costs in terms of individuals' privacy and rights, thus helping to inform decisions regarding which services merit what volume of data.
- developing and adopting a transparent ethics framework to guide data legislation.

Corporate trust measures. Trust in corporations could be measured in a similar manner to trust in government, providing useful insights for Latvia's approach to public-private partnerships.

Participatory decision making. In future contexts where data-driven insights become increasingly powerful, decision-making structures must build in the necessary feedback loops and accountability measures to avoid misuse. One way to develop systematic checks and balances could be to foster a leadership approach that allows more room for all parts of an organisation to voice their opinion and question decisions. Research has shown that participatory decision making contributes to more robust decisions and strategies. This approach could be initiated through a training series on participatory decision making for managers from diverse sectors, by offering simulation games on collective decision making in schools, by testing new tools for public consultations (e.g. in collaboration with media partners) or by offering leadership coaching for entrepreneurs.

Strengthen the capacity to access and use personal data, while safeguarding digital security and safety

The scenarios suggest that Latvia's government might wish to review its system for accessing, integrating and analysing digital information in the future. In a more digital world, creating value for citizens will depend partly on the ability of organisations to access and draw insights from rapidly growing quantities of personal data. At the same time, a more integrated and effective government information system also creates profound risks, which must be mitigated with strong safeguards. The same information that is critical for improving services by monitoring and influencing outcomes also provides significant potential for misuse. Latvia, like most countries, is faced with the challenge of advancing two priorities simultaneously: strengthening the effectiveness of the government's digital information system, while at the same time increasing safeguards. A person-centric principle applies in this context: when a person is the source of data, that person has the right to determine when and where that data is used.

Task force on risks of integrated digital information system. An interdisciplinary task force could explore a broad range of current and potential future risks related to building a stronger and more integrated digital information system. This would include:

- considering situations related to both cybersecurity and the potential abuse of the system by users who gain access both illegally and legally
- developing mitigation solutions in collaboration with key stakeholders that would feed into integrated data safeguarding solutions.

Integrated data safeguarding solutions. The scenario discussion re-emphasised the importance of a consolidated, ongoing, adaptive approach to existing and future safeguarding measures. A nationally co-ordinated digital security strategy could include efforts at the technological, institutional, political and cultural level:

- Technological solutions could integrate mechanisms to separate data and store them in multiple locations, mechanisms to control and track access to information, mechanisms to extract only the minimum data required for a given need, and others.

- Institutional solutions could incorporate rigorous and transparent monitoring and auditing of all data use by both internal and external watchdog functions.
- Political solutions could include partnerships with other governments to mutually audit each other's national safeguards.
- Cultural solutions could involve a high degree of awareness among citizens of the risks and signs of abuse, such that the population will not tolerate moves to weaken or remove safeguards.

ICT provision expertise. Latvia could improve the overall quality and interoperability of services it provides by enhancing the skillset and knowledge of officials. This could include identifying new incentives to recruit ICT experts and practitioners, for example on the basis of staff rotations with Latvian companies.

Conclusion

This chapter explored three alternative scenarios for the future of digital transformation and some of the initial implications for Latvia's digital strategy. The chapter is intended as both a complement to the recommendations in the broader report and as a starting point for further analysis and deliberation in Latvia as part of the ongoing process of developing (and redeveloping) resilient, adaptive and successful strategies.

As both this chapter and the broader report demonstrate, Latvia possesses many of the attributes needed to thrive in the digital era. In a context of rapid change and high uncertainty, however, continued success means advancing beyond what was previously considered satisfactory and investing in new practices and capabilities. Core among the requirements for good governance in the 21st century is the capacity to engage systematically with future uncertainties by mainstreaming strategic foresight approaches in government policy making. The OECD encourages government officials and the broader policy community in Latvia to build upon their foresight experience in the Going Digital exercise, in order to continue their forward-looking work both within the digital policy sphere and beyond.

References

Bajgar, M., et al. (2019), "Industry concentration in Europe and North America", *OECD Productivity Working Papers*, No. 18, OECD Publishing, Paris, *https://doi.org/10.1787/2ff98246-en*.

BBC News (2019), "Russia internet: Law introducing new controls comes into force", *www.bbc.com/news/world-europe-50259597*.

Casalini, F. and J. López González (2019), "Trade and cross-border data flows", *OECD Trade Policy Papers*, No. 220, OECD Publishing, Paris, *https://doi.org/10.1787/b2023a47-en*.

CB Insights (2019), "How Google plans to use AI to reinvent the $3 trillion US healthcare industry", *www.cbinsights.com/research/report/google-strategy-healthcare*.

Deschamps, T. (2019), "Google sister company releases details for controversial Toronto project", The Guardian, *www.theguardian.com/world/2019/jun/24/google-toronto-smart-city-sidewalk-project-alphabet-redevelopment*.

Guarascio, F. (2019), "Alarmed by Libra, EU to look into issuing public digital currency: draft", Reuters, *www.reuters.com/article/us-eu-cryptocurrency-regulations/alarmed-by-libra-eu-to-look-into-issuing-public-digital-currency-draft-idUSKBN1XF1VC*.

Hesse, C. (2008), "Mapping the new commons", paper presented at "Governing Shared Resources: Connecting Local Experience to Global Challenges", the 12th Biennial Conference of the International Association for the Study of the Commons, University of Gloucestershire, Cheltenham, United Kingdom, 14-18 July, *http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/304/Mapping_the_NewCommons.pdf*.

Kerr, S.P. et al. (2016), "Global talent flows", *Harvard Business School Working Papers*, No. 17-026, *www.hbs.edu/faculty/Publication%20Files/17-026_a60ac33d-3fd5-4814-a845-137a38066810.pdf*.

KPMG (2017), *Overview of China's Cybersecurity Law*, 2017 KPMG Advisory (China), *https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf*.

Matias, J.N. (2015), "The tragedy of the digital commons", *The Atlantic*, *www.theatlantic.com/technology/archive/2015/06/the-tragedy-of-the-digital-commons/395129*.

Mölleryd, B. (2015), "Development of high-speed networks and the role of municipal networks", *OECD Science, Technology and Industry Policy Papers*, No. 26, OECD Publishing, Paris, *https://doi.org/10.1787/5jrqdl7rvns3-en*.

Nvidia (2020), "Driving innovation", *www.nvidia.com/en-us/self-driving-cars*.

OECD (2018), "Market concentration", issues paper, OECD, Paris, *https://one.oecd.org/document/DAF/COMP/WD(2018)46/en/pdf*.

Shi-Kupfer, K. and M. Ohlberg (2019), "China's digital rise", *MERICS Papers on China*, No. 7, *https://merics.org/en/report/chinas-digital-rise*.

Walljasper, J. (2011), "Elinor Ostrom's 8 principles for managing a commons", *On the Commons*, *www.onthecommons.org/magazine/elinor-ostroms-8-principles-managing-commmons*.

Notes

1. Available at: *https://uidai.gov.in*.
2. Available at: *https://latlit.eu*.

Chapter 3

INFRASTRUCTURES FOR LATVIA'S DIGITAL ECONOMY

Communication policy objectives for Latvia's digital transformation

As part of their digital strategies, almost all OECD countries have established targets to foster access to and use of communication services. These national targets differ in terms of their end dates, speed and the proportion of the population or premises covered (Table 3.1).

Table 3.1. National broadband coverage targets in the OECD

Country	Year	Coverage
Australia	2020	90% of households and businesses with 50 Mbps/5 Mbps (download/upload)
Austria	2020	99% of households with 100 Mbps
Belgium	2020	100% of households with 30 Mbps
Canada	2021[1]	90% of households and businesses with 50 Mbps/10 Mbps and latest mobile technology available to all households, businesses and major roads
Chile	2020	90% of households with 10 Mbps
Colombia	2022	70% of households connected to the Internet, and 32 million subscriptions with speeds higher than 10 Mbps
Czech Republic	2020	100% of households and businesses with 30 Mbps
Denmark	2020	100% of households and businesses with 100 Mbps/30 Mbps
Estonia	2020	100% of households with 30 Mbps and 60% with 100 Mbps or faster
Finland	2015[2]	99% of households, businesses and public offices with 100 Mbps
France	2022	100% of households, businesses and public offices with 30 Mbps
Germany	2025	Full gigabit coverage of all households and businesses
Greece	2020	100% of households with 30 Mbps
Hungary	2018	100% of households with 30 Mbps
Iceland	2020	100% of households with 30 Mbps
Ireland	2020	100% of households with 30 Mbps
Israel	2022	100% of population with 30 Mbps
Italy	2020	100% of households with 30 Mbps; 100% of businesses and 85% of population with 100 Mbps
Korea	2022	Fixed internet with maximum 10 Gbps download speeds will be disseminated to 50% of urban households (85 cities) by 2022
Latvia	2020	100% of population with 30 Mbps mobile broadband and 100% of rural areas with optical backhaul
Luxembourg	2020	100% of households, businesses and public offices with 1 Gbps/500 Mbps
Netherlands	2020	100% of households with 30 Mbps
New Zealand	2025	99% of households with 50 Mbps and the remaining 1% with 10 Mbps
Norway	2020	90% of households with 100 Mbps
Poland	2020	100% of households and businesses with 30 Mbps
Portugal	2020	100% of households with 30 Mbps
Slovak Republic	2020	100% of households with 30 Mbps
Slovenia	2021	96% of households with 100 Mbps and the remaining 4% with 30 Mbps
Spain	2020	100% of households with 30 Mbps
Sweden	2025	98% of households and businesses with 1 Gbps
Switzerland	2020	100% of municipalities with 30 Mbps
United Kingdom	2020	95% of households and businesses with 25 Mbps
United States	2020	80% of households with 100 Mbps/50 Mbps

1. By the end of 2021, with the remaining 10% to be achieved within 10 to 15 years.

2. A national broadband strategy currently under development will define targets for the years 2025 and 2030.

Note: Mbps = megabits per second; Gbps = gigbits per second.

Sources: OECD (2018a), "Bridging the rural digital divide", *https://dx.doi.org/10.1787/852bd3b9-en*; DEO 2020 regulatory questionnaire.

Latvia aims to connect 100% of the population to 30 Mbps mobile broadband services and to deploy fibre backhaul in all rural areas by 2020. These targets are included in Latvia's 2018-2020 national policy plan for the communication sector and are aligned with the high-speed Internet coverage targets of the Digital Agenda for Europe for 2020. As for all other EU countries, the minimum common target is to achieve 100% coverage with 30 Mbps and 50% of households with broadband subscriptions of 100 Mbps by 2020 (European Commission, 2010).

The benchmark of 30 Mbps connectivity is now a common standard, though targets of at least 100 Mbps are becoming increasingly frequent. By 2020, the United States aims to have broadband of 100 Mbps or more available to 80% of households, while Norway and Austria have set targets of 90% and 99%, respectively. Some targets are even more ambitious, such as the 1 Gbps target of Luxembourg (98% by 2020) and (100% by 2025) and Korea's target of 10 Gbps download speeds for 50% of urban households by 2022 (OECD, 2018a).

OECD countries also have established connectivity targets related to public service providers and mobility. The gigabit society objectives of the European Commission (EC) are: 1) to ensure that all schools, transport hubs and main providers of public services, as well as digitally intensive enterprises, have access to Internet connections with download/upload speeds of 1 Gigabit of data per second; 2) all households, rural or urban, have access to networks offering a download speed of at least 100 Mbps, which can be upgraded to 1 Gigabit; and 3) all urban areas, as well as major roads and railways, have uninterrupted 5G wireless broadband coverage (European Commission, 2016).

Latvia's connectivity targets are based on its national broadband strategy, "Next Generation Access Network Development 2013–2020", which was approved by the Cabinet of Ministers of the Republic of Latvia in December 2012 and amended in 2016. The two major priorities of the plan are the development of a fibre backhaul infrastructure (middle-mile) for wholesale broadband services, including in rural areas, and the roll-out of 4G network services across the country. The national broadband strategy and its targets are monitored by the Ministry of Transport (MoT) and submitted for approval to the Cabinet of Ministers every two years. A key challenge affecting implementation of the strategy of Latvia relates to the expansion of connectivity in rural areas, as a result of low incomes in these areas and population density. An additional challenge is the lack of available funds for last-mile connectivity.

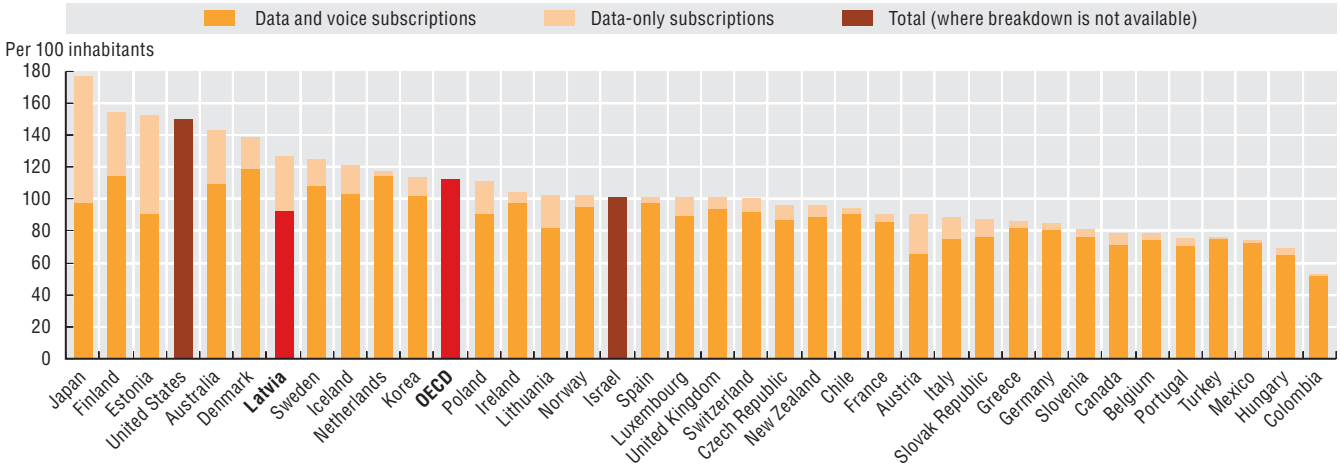
For its next broadband policy strategy covering the post-2020 period, the government plans to continue network deployment in rural areas, including by expanding middle and last-mile coverage. It is also expected that the post-2020 strategy will incorporate extensive mapping of communication networks and services to facilitate deployment of 5G networks and infrastructure sharing. The MoT is currently working to identify funding sources and the government plans to finalise the new strategy by end 2020.

State of connectivity in Latvia

Broadband penetration

Mobile broadband subscriptions have continued to grow in Latvia, as in most OECD countries. From December 2017 to December 2018, subscriptions grew by 11%, and in June 2019 reached 126.9 subscriptions per 100 inhabitants, which places Latvia 7th among OECD countries (Figure 3.1).

Figure 3.1. Mobile broadband subscriptions per 100 inhabitants in OECD countries, June 2019

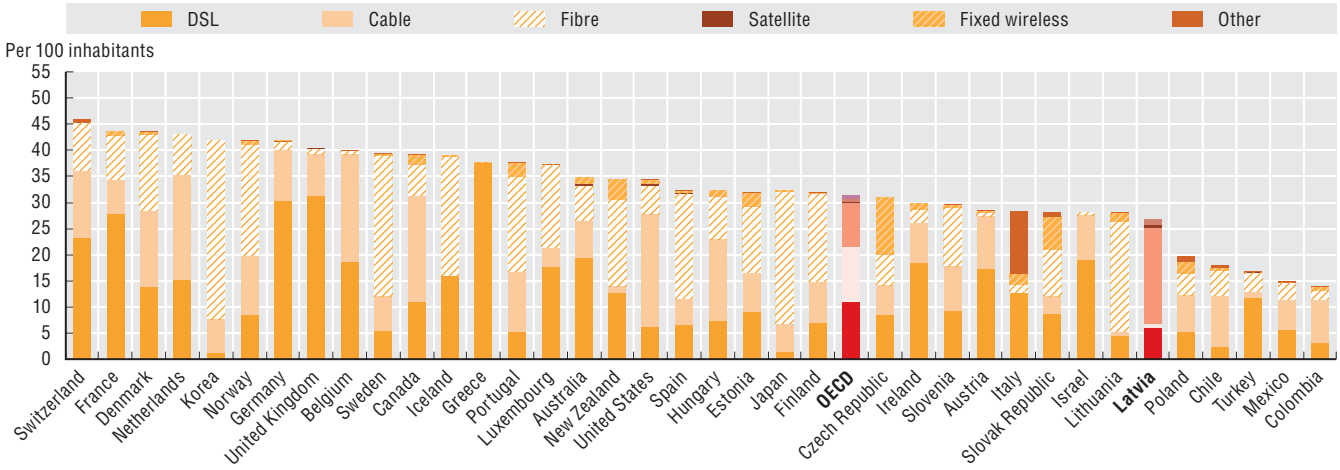


Note: Australia: Data reported for December 2018 and onwards are being collected by a new entity using a different methodology. Figures reported from December 2018 comprise a series break and are non-comparable with previous data for any broadband measures reported by Australia to the OECD.

Source: OECD (2020b), *OECD Broadband Portal* (database), *www.oecd.org/sti/broadband/oecdbroadbandportal.htm* (accessed on 6 May 2020).

In June 2019, Latvia reported 26.7 fixed broadband subscriptions per 100 inhabitants, close to the OECD average of 31.4. However, Latvia lags substantially behind leading OECD countries in terms of fixed broadband penetration, such as Switzerland with 46 and Denmark with 43 subscriptions per 100 inhabitants (Figure 3.2).

Figure 3.2. Fixed broadband subscriptions per 100 inhabitants in OECD countries, June 2019

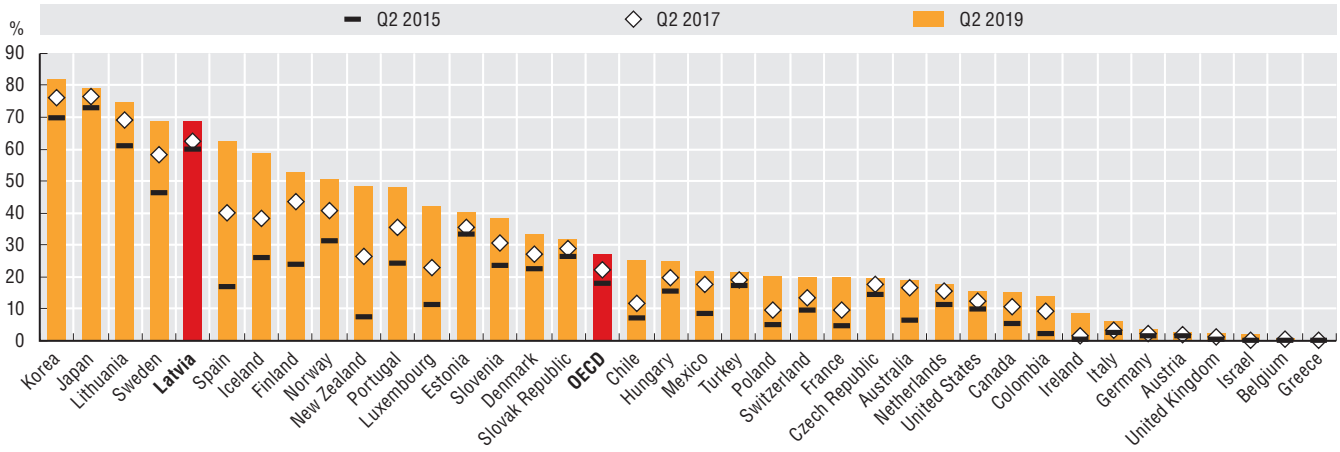


Notes: DSL = digital subscriber line. Australia: Data reported for December 2018 and onwards are being collected by a new entity using a different methodology. Figures reported from December 2018 comprise a series break and are non-comparable with previous data for any broadband measures reported by Australia to the OECD. The OECD definition of fibre differs substantially from fibre classifications commonly used in Australian reporting. These figures treat connections known in Australia as "fibre-to-the-node" and "fibre-to-the-curb" as DSL connections, while "fibre-to-the-premises" and "fibre-to-the-basement" are treated as fibre connections. Data on technology type prior to Q2 2016 should be treated as indicative until further notice.

Source: OECD (2020b), *OECD Broadband Portal* (database), *www.oecd.org/sti/broadband/oecdbroadbandportal.htm* (accessed on 6 May 2020).

The percentage of fibre connections in total fixed broadband reached 68.9% in Latvia in June 2019, much higher than the OECD average of 26.8% (Figure 3.3). From 2009 to June 2019, the share of fibre subscriptions among overall fixed broadband subscriptions in Latvia increased exponentially from 5% to 68.5%, (Figure 3.4). In June 2019, Latvia ranked fifth in terms of percentage of fibre connections in total fixed broadband, after Korea (81.6%), Japan (79.0%) and Lithuania (74.6%).

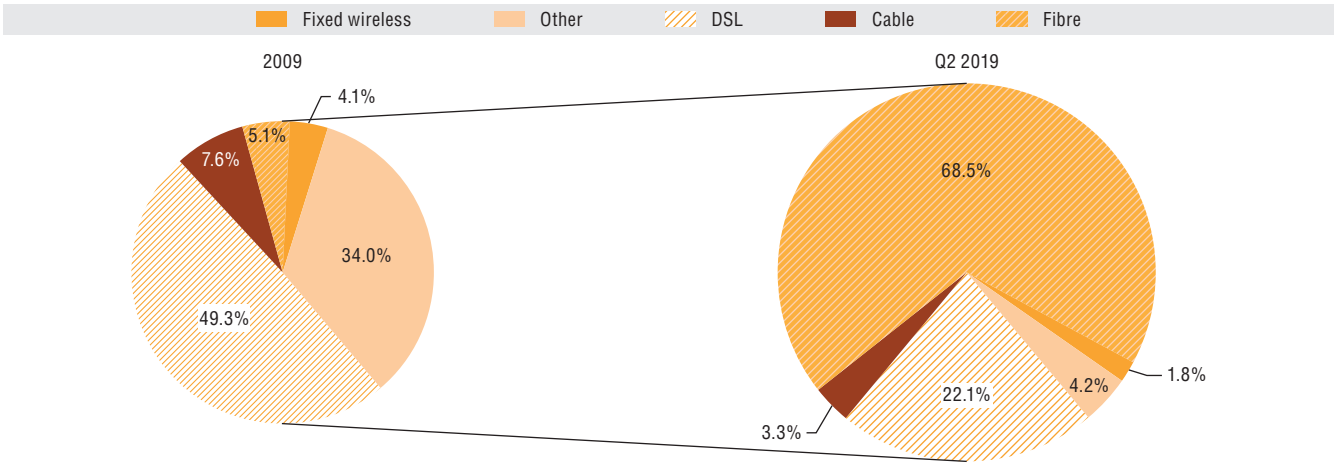
Figure 3.3. Percentage of fibre connections in total fixed broadband in OECD countries, Q2 2015 – Q2 2019



Notes: Australia: Data reported for December 2018 and onwards are being collected by a new entity using a different methodology. Figures reported from December 2018 comprise a series break and are non-comparable with previous data for any broadband measures reported by Australia to the OECD. The OECD definition of fibre differs substantially from fibre classifications commonly used in Australian reporting. These figures treat connections known in Australia as "fibre-to-the-node" and "fibre-to-the-curb" as DSL connections, while "fibre-to-the-premises" and "fibre-to-the-basement" are treated as fibre connections. Data on technology type prior to Q2 2016 should be treated as indicative until further notice. Data for Israel are OECD estimates. Data for Switzerland and United States are preliminary.

Source: OECD (2020b), *OECD Broadband Portal* (database), *www.oecd.org/sti/broadband/oecdbroadbandportal.htm* (accessed on 6 May 2020).

Figure 3.4. Fixed broadband subscriptions in Latvia, by technology, 2009 – Q2 2019

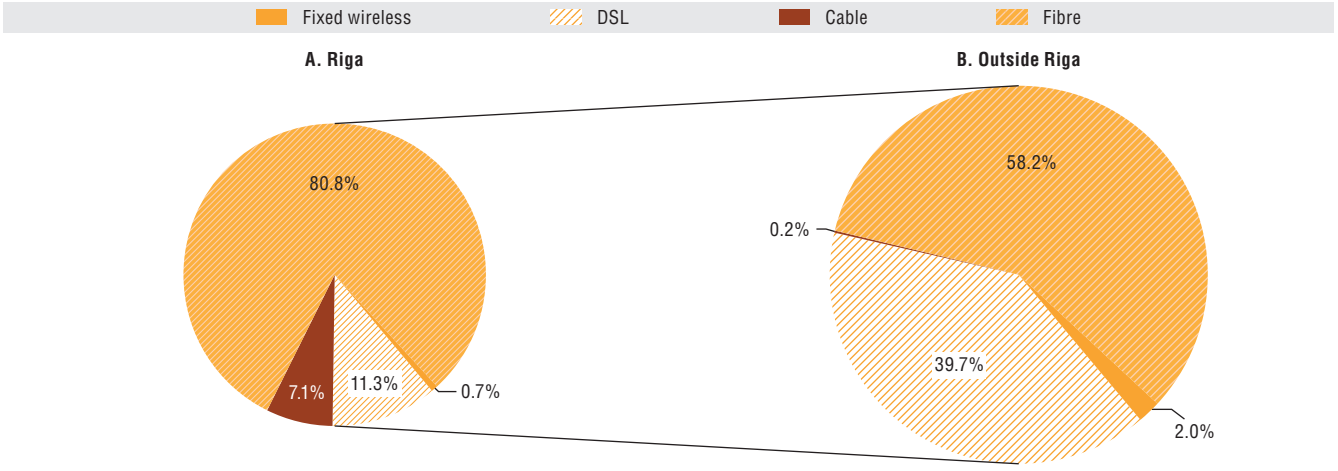


Notes: DSL = digital subscriber line. Satellite subscriptions were negligible in Latvia in 2009 (around 0.01% of the total) and non-existent as of June 2019.

Source: OECD (2020b), *OECD Broadband Portal* (database), *www.oecd.org/sti/broadband/oecdbroadbandportal.htm* (accessed on 6 May 2020).

However, differences persist between urban and rural areas in Latvia, particularly when comparing Riga to other regions. While fibre accounts for 80.8% of connections in Riga, the number falls to 58.2% outside the capital (Figure 3.5). Such regional variation, coupled with the fact that almost 20% of households in rural areas lack fixed broadband connections at speeds of over 30 Mbps (Figure 3.8), point to the substantial connectivity gap in high-quality communication services that still exists between urban and rural areas in Latvia. Bridging this gap will be critical to advance Latvia's digital transformation of the economy and society in an inclusive manner.

Figure 3.5. Fixed broadband subscriptions in Riga and outside Riga, by technology, 2018



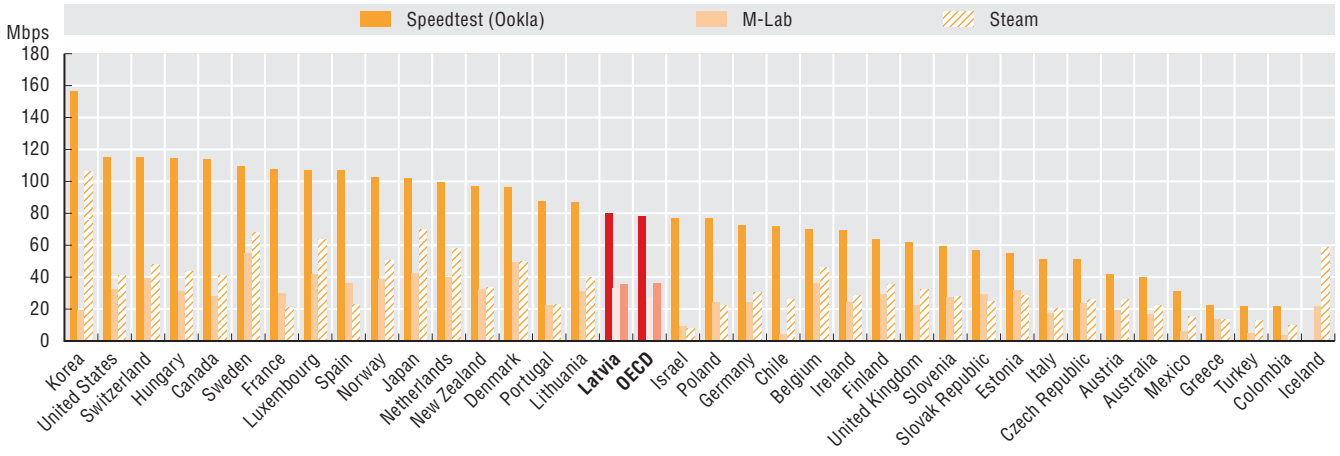
Notes: DSL = digital subscriberline. Data as of December 2018.

Source: OECD, based on SPRK information.

Broadband speeds

Multiple sources of speed tests allow for a range of measured download speeds of broadband services. Three different sources are used in this section: Ookla and M-Lab provide a broader view on networks, while the online gaming platform Steam measures the speeds of its users. According to Ookla, Latvia ranks 17th for broadband services among OECD countries, with an average actual download speed of 79.8 Mbps, compared to the OECD average of 78.3 Mbps in July 2019 (Ookla, 2019). Average download speeds of fixed broadband connections collected by M-Lab and Steam rank Latvia 12th and 16th among OECD countries, with 32.7 Mbps and 35.7 Mbps, respectively (Figure 3.6).

Figure 3.6. Average experienced download speeds of fixed broadband connections in OECD countries, July 2019

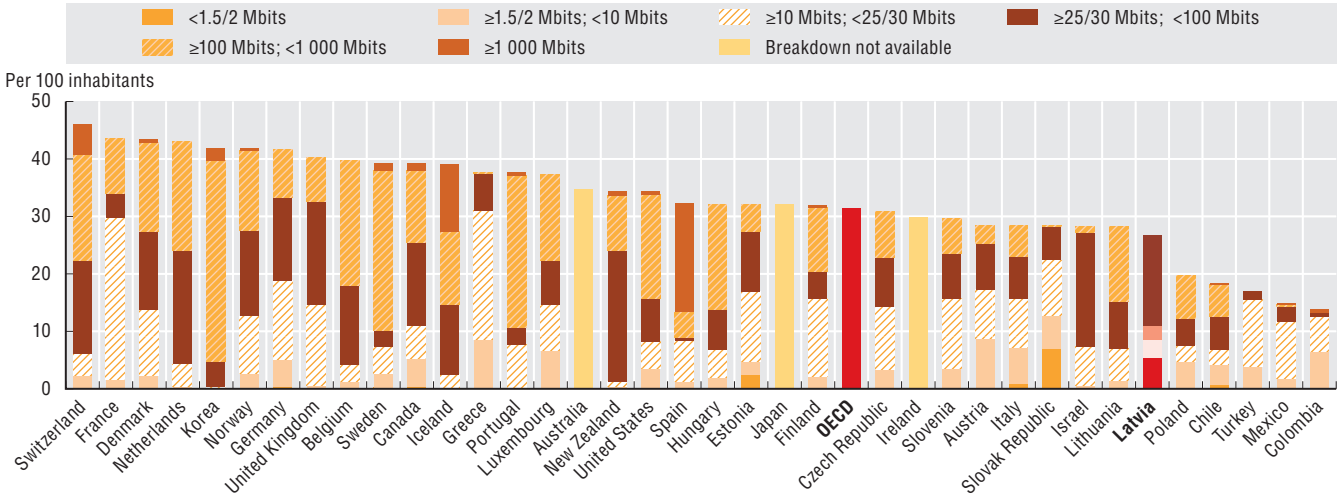


Notes: Mbps = megabits per second. Speedtest (Ookla) data are for July 2019. M-Lab speeds were measured over the period 9 May 2018 to 8 May 2019. Steam data are for July 2019.

Sources: Ookla (2019), "Speedtest", *www.speedtest.net/global-index* (accessed on 9 May 2020); M-Lab (2019), "Worldwide broadband speed league", *www.cable.co.uk/broadband/speed/worldwide-speed-league* (accessed on 9 May 2020); Steam (2019), "Steam download stats", *https://store.steampowered.com/stats/content* (accessed on 9 May 2020).

In terms of subscriptions per advertised speed tiers, Latvia shows a high proportion of fixed broadband subscriptions for contracted speeds of over 100 Mbps. These subscriptions represent 59% of total fixed broadband subscriptions, or 16 subscriptions per 100 inhabitants (Figure 3.7).

Figure 3.7. Fixed broadband subscriptions per 100 inhabitants in OECD countries, by speed tier, June 2019

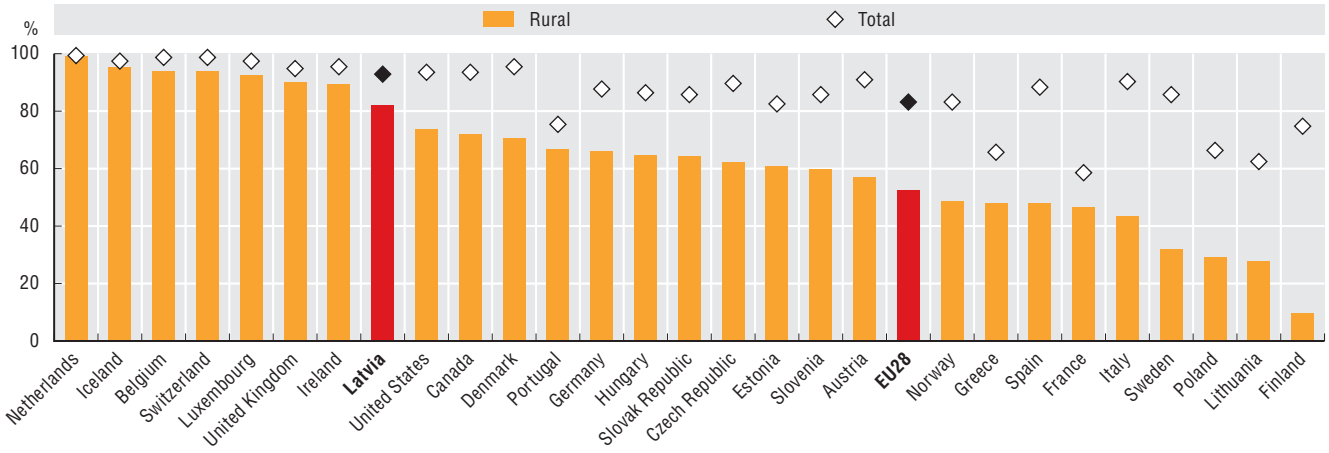


Notes: Mbit = megabits per second. Switzerland and United States: Data for June 2019 are estimates.

Source: OECD (2020c), *OECD Broadband Portal* (database), *www.oecd.org/sti/broadband/oecdbroadbandportal.htm* (accessed on 6 May 2020).

While Latvia has made progress in ensuring the availability of high-speed fixed broadband in its territory, gaps exists in terms of coverage (i.e. connections over 30 Mbps) in rural and remote areas in the country. In 2018, while 93% of Latvian households in the total territory were located in areas (i.e. including both rural and urban areas) with availability of fixed broadband connections of speeds above 30 Mbps, coverage in rural areas of similar services was 82.1%, a difference of about 11 percentage points. Coverage in Latvia of fixed broadband over 30 Mbps is well above the European average (EU28) of 83.2% in total territory and only 52.3% in rural areas, but lags behind leading OECD countries such as the Netherlands, Iceland, Belgium, Switzerland and the United Kingdom (Figure 3.8).

Figure 3.8. Percentage of households in total and rural areas[1] with minimum 30 Mbps of fixed broadband coverage[2] in selected OECD countries, June 2018

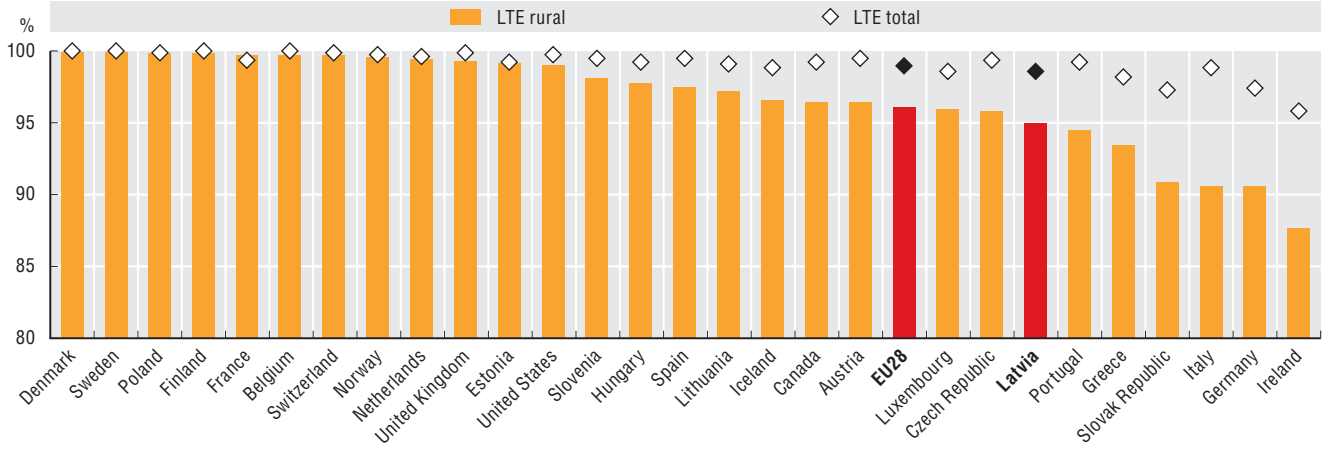


1. For EU countries, rural areas are those with a population density less than 100 per square kilometre. For Canada, rural areas are those with a population density less than 400 per square kilometre. For the United States, rural areas are those with a population density less than 1 000 per square mile or 386 people per square kilometre.
2. For EU countries, coverage of NGA technologies (VDSL, FTTP, DOCSIS 3.0) capable of delivering at least 30 Mbps download was used. For the United States, coverage of fixed terrestrial broadband capable of delivering 25 Mbps download and 3 Mbps upload services was used; data refer to 2016.

Source: OECD calculations based on CRTC (2019), *Communications Monitoring Report*, *https://crtc.gc.ca/eng/publications/reports/policymonitoring/2019/index.htm*; European Commission (2018a), *Study on Broadband Coverage in Europe*, *https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62760*; FCC (2019), *Broadband Deployment Report*, *www.fcc.gov/reports-research/reports/broadband-progress-reports/2019-broadband-deployment-report*.

For high-speed, long-term evolution (LTE) mobile coverage in rural areas, however, Latvia's performance is below the European (EU28) average. The EU28 average for LTE coverage is 96.1% in rural areas, with leading countries such as Denmark and Sweden reporting 100% LTE coverage in these areas; however, only 95% of rural areas are covered by LTE in Latvia, in comparison to 98.6% of urban areas (Figure 3.9).

Figure 3.9. Percentage of households with LTE mobile coverage, total and rural areas[1] in selected OECD countries, June 2018



1. For EU countries, rural areas are those with a population density less than 100 per square kilometre. For Canada, rural areas are those with a population density less than 400 per square kilometre. For the United States, rural areas are those with a population density less than 1 000 per square mile or 386 people per square kilometre.

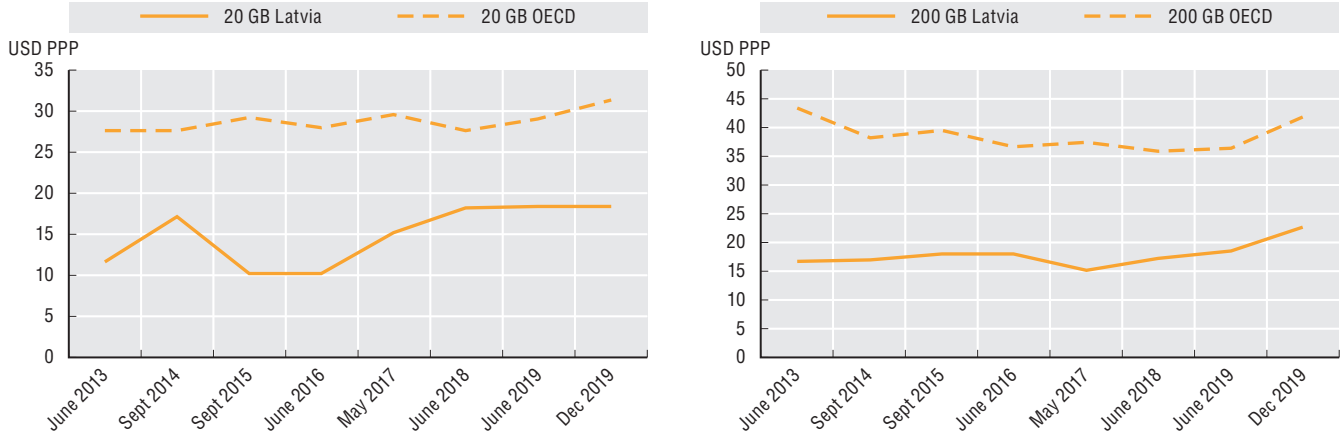
Note: LTE = long-term evolution.

Source: OECD calculations based on CRTC (2019), *Communications Monitoring Report*, *https://crtc.gc.ca/eng/publications/reports/policymonitoring/2019/index.htm* ; European Commission (2018a), *Study on Broadband Coverage in Europe*, *https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62760*; FCC (2019), *Broadband Deployment Report*, *www.fcc.gov/reports-research/reports/broadband-progress-reports/2019-broadband-deployment-report*.

Prices of fixed and mobile broadband services

Prices for fixed broadband connectivity in Latvia are substantially lower than the OECD average in both "low-usage" (20 GB) and "high-usage" (200 GB) fixed broadband baskets. In December 2019, prices for both "low usage" (20 GB) and "high usage" (200 GB) levelled closely at USD PPP 18.38 and USD PPP 22.59, respectively, while the OECD averages were USD PPP 31.33 and USD PPP 41.80 for each basket. While average prices across the OECD for fixed broadband access appear to have declined between 2013 and 2019, the same trend was not observed in Latvia. During the same period, prices for "high-usage" baskets of fixed broadband offers increased slightly from USD PPP16.83 to the current level of USD PPP 22.89, whereas "low-usage" fixed broadband baskets have increased from USD PPP 11.71 to USD PPP 18.38 (Figure 3.10).

Figure 3.10. Trends in fixed broadband prices in Latvia and OECD countries, June 2013-December 2019

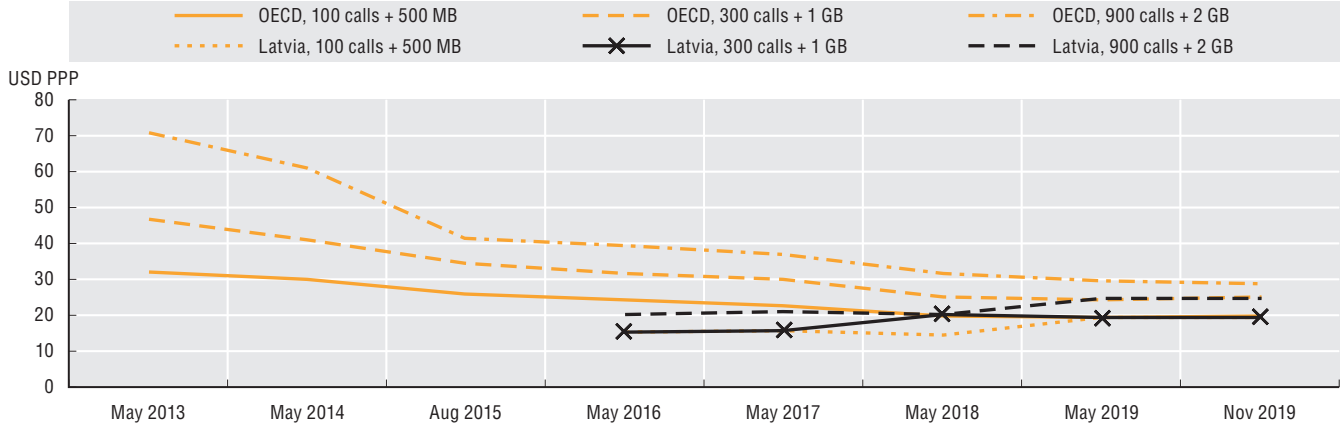


Notes: PPP = purchasing power parity; GB = gigabyte. Data as of December 2019.

Source: OECD calculations based on data provided by Strategy Analytics.

With regard to mobile connectivity, prices for mobile broadband services in Latvia for "low-usage" and "high-usage" baskets are also lower than the OECD averages, although the difference between Latvia's price levels and OECD averages is smaller than with respect to fixed broadband baskets. Available data from 2016 to 2019 show pronounced increases in prices for all baskets. For both the "low-usage" basket (100 calls + 500 MB) and "medium-usage" basket (300 calls + 1 GB), prices increased from USD PPP 15.37 in 2016 to USD PPP 19.32. For the "high-usage" basket (900 calls + 2 GB), prices increased from USD PPP 20.11 to USD PPP 24.58 (Figure 3.11).

Figure 3.11. Trends in mobile broadband prices in Latvia and OECD countries, May 2013-November 2019



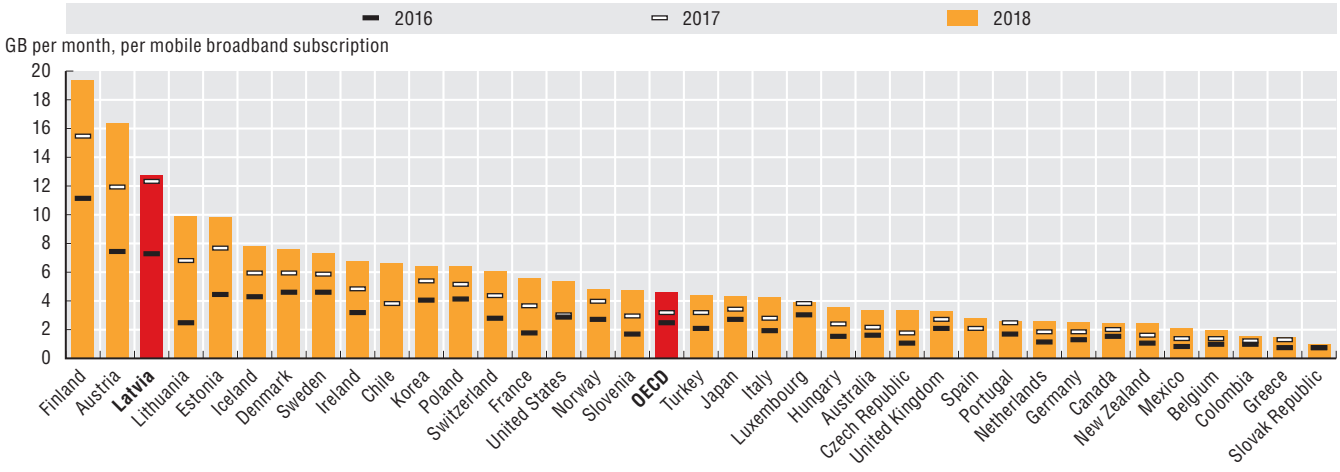
Notes: PPP = purchasing power parity; MB = megabyte; GB = gigabyte. Data as of November 2019.

Source: OECD calculations based on Strategy Analytics data.

Mobile data usage

In 2018, mobile data usage per mobile broadband subscription in Latvia was 12.8 GB per month. Latvia's average monthly mobile data usage is much higher than the OECD average of 4.7 GB per month and lags behind only Finland and Austria, where data usage per subscription each month amounts to 19.4 GB and 16.4 GB, respectively (Figure 3.12). Increases in mobile data usage reflect a growing demand for network capacity.

Figure 3.12. Mobile data usage per mobile broadband subscription in OECD countries, 2016-18



Notes: GB = gigabyte. Australia: Data reported for December 2018 and onwards are being collected by a new entity using a different methodology. Figures reported from December 2018 comprise a series break and are non-comparable with previous data for any broadband measures reported by Australia to the OECD. Data for Switzerland are preliminary.

Source: OECD (2020b), *OECD Broadband Portal* (database), *www.oecd.org/sti/broadband/oecdbroadbandportal.htm* (accessed on 6 May 2020).

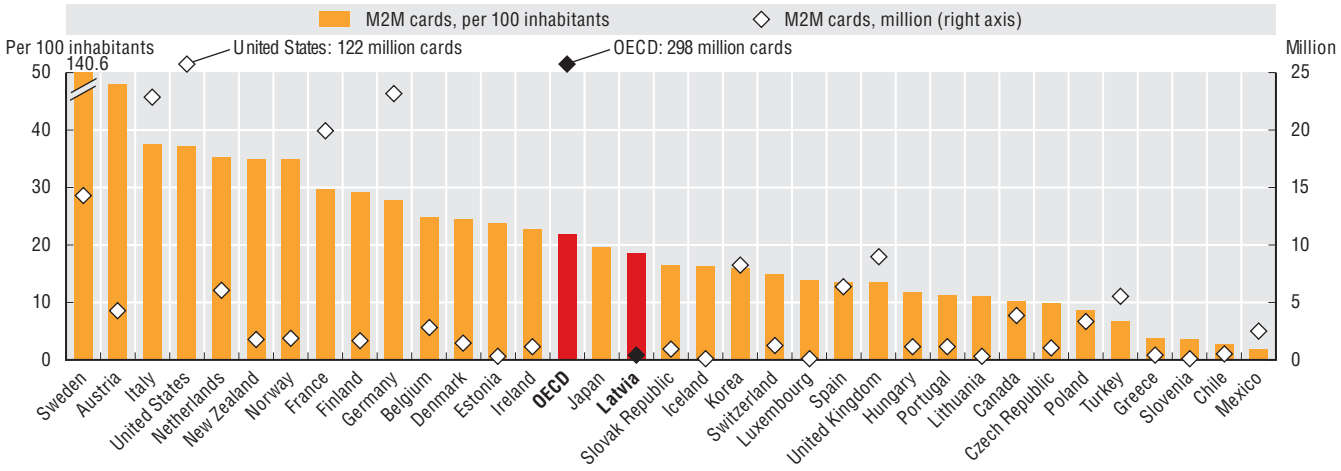
The Internet of Things

The Internet of Things (IoT) represents the next step in the convergence of information and communication technologies (ICTs), societies and the economy. While the effects of the IoT on growth and productivity is yet to be measured systematically across OECD countries (OECD, 2019a), the IoT has the potential to contribute to local and national goals of innovation and efficiency. In order to achieve those goals, communication technologies and other enablers must be available to support data flows.

In Latvia, three mobile and three fixed operators provide Machine-to-machine (M2M) subscriptions – a subset of the IoT. As of June 2019, in terms of M2M embedded devices, Latvia had 18.5 M2M cards per 100 inhabitants (i.e. 360 000 M2M cards in total). Latvia's performance in terms of M2M penetration is just below the OECD average of 22%; however, it lags behind OECD leaders such as Sweden (140.6%), Austria (48.2%), Italy, (37.7%), the United States (37.3%) and others (Figure 3.13). Nevertheless, it is important to note that M2M data in some OECD countries, such as Sweden, may include devices that might be located in other countries (e.g. SIM cards in automobiles). The regulator in Latvia (SPRK) does not collect information regarding operators' provision of M2M devices for foreign use.

In Latvia, discussions are underway regarding a new numbering range for M2M communications. Under the existing regulation, operators offer IoT/M2M services based on mobile numbering resources allocated to them. Although the current numbering plan states that the allocation of additional numbering resources for M2M services is unnecessary, a forthcoming MoT report suggests a change in the national numbering plan. This new proposal plans to allocate an 11-digit numbering resource for IoT/MSM for extraterritorial use as well as an 8-digit number for local use, and gradually implement a fee for all numbering resources, which are currently distributed without a charge.

Figure 3.13 M2M/embedded mobile cellular subscriptions in selected OECD countries, June 2019



Note: The OECD defines machine to machine (M2M) on mobile networks as "the number of SIM cards that are assigned for use in machines and devices (cars, smart meters and consumer electronics) and are not part of a consumer subscription". This means that dongles for mobile data and tablet subscriptions should be counted by countries under the mobile broadband definition, whereas SIM cards in personal navigation devices, smart meters, trains, automobiles and so on should be counted under the M2M category. Australia: Data reported for December 2018 and onwards are being collected by a new entity using a different methodology. Figures reported from December 2018 comprise a series break and are non-comparable with previous data for any broadband measures reported by Australia to the OECD. Data for Switzerland are preliminary. Data for the United States are OECD temporary estimates.

Source: OECD (2020b), *OECD Broadband Portal* (database), *www.oecd.org/sti/broadband/oecdbroadbandportal.htm* (accessed on 6 May 2020).

Going forward, it will be important to ensure proactive policy development for IoT in order to align different sectoral, national and subnational objectives in Latvia. The government will play a key role in engaging with the private sector and local stakeholders to develop solutions for local challenges and IoT capacity, and to help drive demand for IoT services, while also ensuring there is regulatory balance and that digital security and privacy risks are managed.

Internet exchange points

A well-functioning communication infrastructure includes efficient exchange of Internet traffic. Internet exchange points (IXPs) are important to keep traffic local (Weller and Woodcock, 2013). IXPs are also key for international Internet traffic, because they foster efficient traffics exchange domestically. Traffic originating and terminating domestically can and should be routed domestically. Routing this same traffic via other countries increases latency and costs and is often indicative of sub-optimal development of the Internet traffic exchange market in a given country.

Latvia has three IXPs: the Santa Monica Internet Local Exchange (SMILE, established in 2005), the Latvian Internet Exchange (LIX, established in 2007) and the most recently established, MSK-IX (established in 2018) in Riga. The largest IXP in terms of members is SMILE.

LIX is owned by three Internet service providers (ISPs): Tet (previously Lattelecom), Latnet and Telia Latvija. The management of this IXP does not seem to follow best international practices. For example, LIX limits traffic to Latvian prefixes, effectively preventing networks from optimising interconnections with international players. This rather closed design of the exchange hinders long-term traffic growth as well as the growth of entities exchanging traffic at this exchange. Moreover, LIX uses a layer 3 design (routing packets instead of switching frames) which is less cost effective and prevents networks from generating bilateral peering sessions. In contrast, competitive and dynamic IXP ecosystems provide the infrastructure for network operators to peer and exchange traffic at their own convenience.

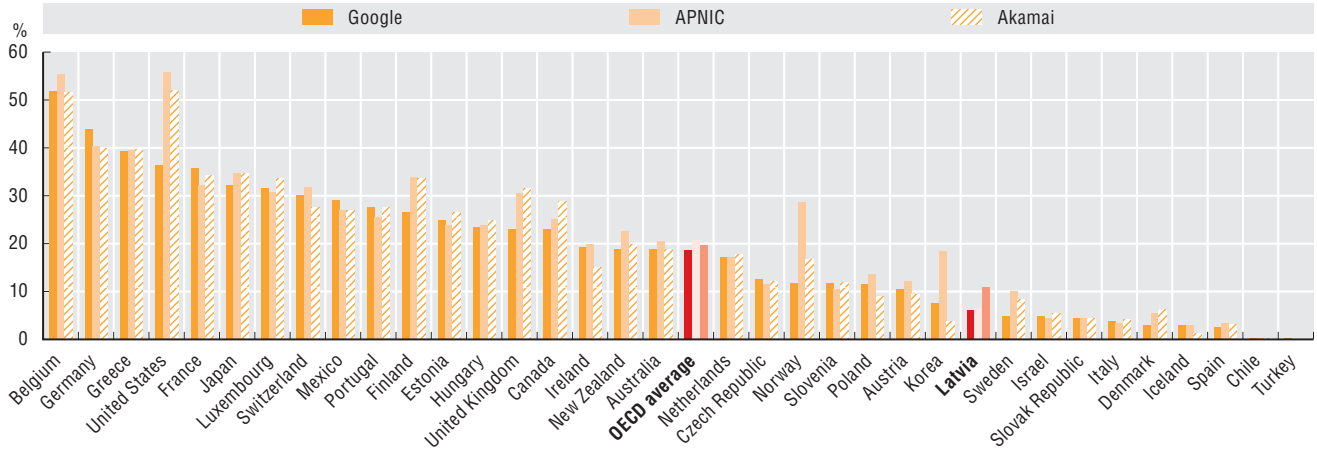
From a pricing perspective, the monthly cost for a 10 Gigabit port with LIX (i.e. the overhead costs of peering inherent to transit costs) is quite high in comparative terms. The price for 40% utilisation of a 10 Gigabit Ethernet link, per month, is EUR 0.53/Mbps. In comparison, the price in Amsterdam (AMS-IX) is EUR 0.18/Mbps, and the price in Moscow (MSK-IX) is EUR 0.29/Mbps.[1] Prices for SMILE and MSK-IX are not publicly available.

IXP performance is not monitored by SPRK as this task falls outside the mandate of the communication regulator. SPRK is responsible only for broadband quality measurements from network termination point up to IXPs, where the regulator's measurement servers have been collocated. A dedicated analysis of the state of traffic exchange in Latvia could help identify existing challenges and design potential solutions, and if conducted in partnership with stakeholders, could further improve IXP performance and increase the amount of traffic exchanged locally.

One potential challenge for the future of the Internet is the ability to connect tens of billions of devices. A key resource needed not only to ensure scalability, but also to increase security, is the new version of the Internet Protocol (IP), IPv6, which replaces its largely exhausted IP predecessor, IPv4, in terms of the distribution of unassigned addresses. Encouraging the deployment of IPv6 has been a long-standing goal for OECD countries. However, its adoption has been slower than expected, which may hinder the development of new applications and services (OECD, 2014; 2018b).

Regarding IPv6 adoption, multiple sources show that Latvia is significantly behind the OECD average. According to Google data, for example, IPv6 adoption reached 6.7% in June 2020, against the OECD average of 22.4%. In the same period, the rate in Belgium and Germany, both OECD leading countries in IPv6 adoption, was 55.7% and 49.7%, respectively (Figure 3.14). Data from APNIC and Akamai from June 2020 indicate that IPv6 adoption in Latvia was 6.9% and 10.3%, respectively, while OECD averages were 24.4% and 23.5%. In order to encourage the adoption of IPv6, the new Cybersecurity Strategy for 2019-2022 has set a target of the end of 2020 for the MoT and the Ministry of Environmental Protection and Regional Development (VARAM) to implement a set of measures fostering the use of IPv6 in ICT equipment used by the public sector.

Figure 3.14. IPv6 adoption in selected OECD countries, 2020



Sources: Google, 2020, "Per-country IPv6 adoption", *www.google.com/intl/en/ipv6* (accessed in June 2020); APNIC (2020), "IPv6 measurement maps", *http://stats.labs.apnic.net/ipv6* (accessed in June 2020); Akamai (2020), "IPv6 adoption visualization", *www.akamai.com/uk/en/our-thinking/state-of-the-internet-report/state-of-the-internet-ipv6-adoption-visualization.jsp* (accessed in June 2020).

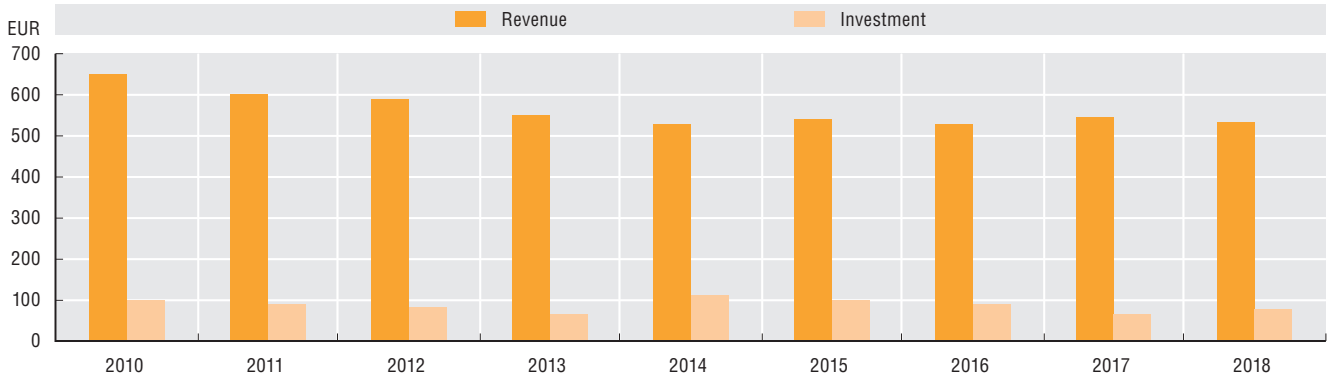
Developments in communication markets in Latvia

Since 2013, revenues in the communication sector have been stable. By 2018, total revenue and investment in the communication sector in Latvia amounted to EUR 532 million and EUR 78 million, respectively (Figure 3.15).

The communication sector in Latvia comprises a multitude of market players, offering services in both fixed and mobile markets. In the retail market, there are three main players in the fixed market and four different players in the mobile market (Table 3.2).

In the wholesale market, the fully state-owned operator, LVRTC, provides wholesale broadband services, as well as towers and masts. Beyond broadband services, LVRTC offers cloud, e-signature and digital security services. LVRTC is also responsible for registering and maintaining the "gov.lv" domain name.[2] Aside from LVRTC, four other wholesale-only operators in Latvia offer national and international gateway services to other companies in the market.

Figure 3.15. Trends in communication revenue and investment in Latvia, 2010-18



Source: OECD (2020a), *OECD Telecommunications and Internet Statistics* (database), *https://doi.org/10.1787/data-00170-en* (accessed on 9 July 2020).

Table 3.2. Main players in the Latvian communication markets

Communication player	Markets	Ownership structure
LVRTC	Wholesale-only broadband services and TV and radio broadcasting	Latvian government (100%)
Tet (previously Lattelecom)	Fixed incumbent offering fixed voice, fixed broadband, pay TV and electricity	Latvian government (51%) and Telia (49%)
Baltcom	Fixed voice, fixed broadband, pay TV and electricity	Rpax One S.A. (96.4%)
Balticom	Fixed voice, fixed broadband, pay TV	Privately owned
CSC	Fixed voice and fixed broadband	Privately owned
LMT	Mobile and fixed wireless services[1]	Sonera Holding (24.5%), Telia (24.5%), Tet (23%), LVRTC (23%) and Latvian government (5%)
Tele2	Mobile	Tele2 Sverige Aktiebolag (100%)
Bite	Mobile	BITE Lietuva UAB (100%)
Triatel	Mobile	Telekom Baltija
Zetcom (Amigo)[2]	Mobile	X

1. LMT is a mobile operator, which offers fixed-wireless services including voice and broadband services through mobile technologies.

2. The Amigo brand, operated by Zetcom, ceased operations in June 2019, and the customers were taken over by LMT.

Note: x = not applicable.

There were 278 communication operators registered by SPRK as of December 2018, indicating a reduction of 12% in comparison to 2017. Out of all service providers, 65% provide broadband access services (SPRK, 2018).

Fixed market developments

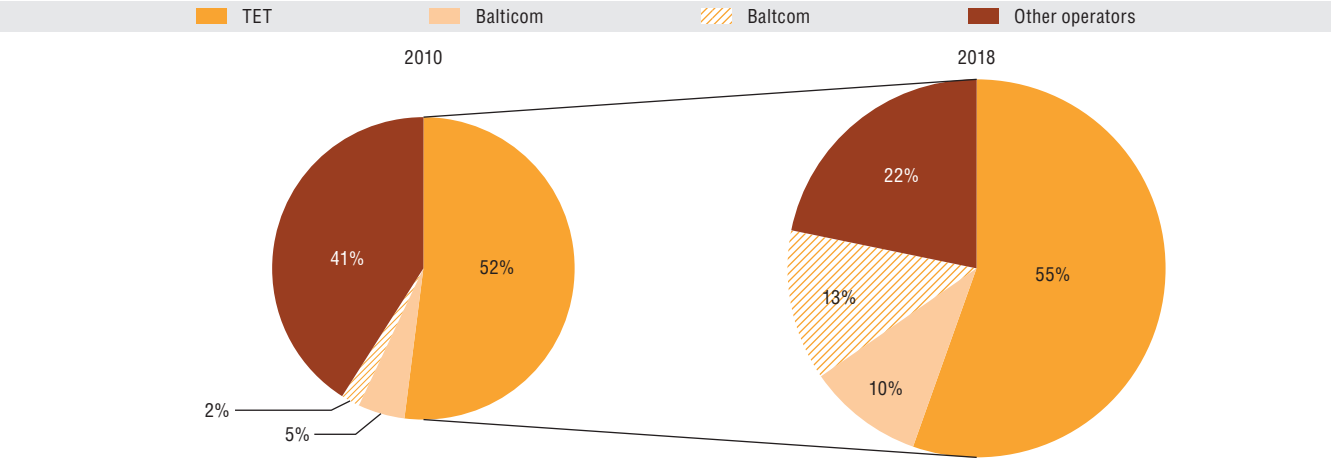
In Latvia, Tet (until April 2019 branded as Lattelecom) is the historical incumbent. The operator owns a nationwide infrastructure and is the largest fixed broadband provider. Alternative fixed broadband providers (cable operators and ISPs) started to deploy their own infrastructure following liberalisation in 2003, and have concentrated on fibre deployment, investing first in urban areas and focusing on fibre-to-the-building (FTTB). Fibre deployment has since expanded to less densely populated areas where a business case for investment has been identified.

In response, Tet started investing in fibre-to-the-home (FTTH) in 2006. Currently, Tet is the main FTTH provider competing with alternative FTTB providers. In 2014, Tet started to deploy VDSL2 vectoring technology to improve the performance of its copper network. Such infrastructure competition has been the main driver behind the development of fibre access networks in Latvia.

Entries and exits in the fixed market by very small operators are relatively frequent (European Commission, 2019). In December 2018, Tet accounted for 56% of fixed broadband subscriptions, while

Baltcom accounted for 13%, Balticom for 10% and other operators for 22%. This latter share includes 154 operators, the majority of which are small operators (Figure 3.16). Tet's market share has increased in relation to 2010, when it held 52%, but has decreased from 58.8% in July 2015. However, it is still higher than the average market share for incumbents in the European Union (40.3%) (European Commission, 2018b). Recently the number of "other operators" has been decreasing due to mergers. It should be noted, however, that Latvia does not have a defined criteria as to what constitutes a "small operator".

Figure 3.16. Fixed broadband market shares in Latvia, 2010 and 2018



Source: SPRK (2018a), *Elektronisko sakaru nozares: faktos un skaitlos 2018* [Electronic communications sectors: facts and figures 2018], *https://infogram.com/id-es_nozares_raditaji_2018-1hxj48qk0y154vg?live*.

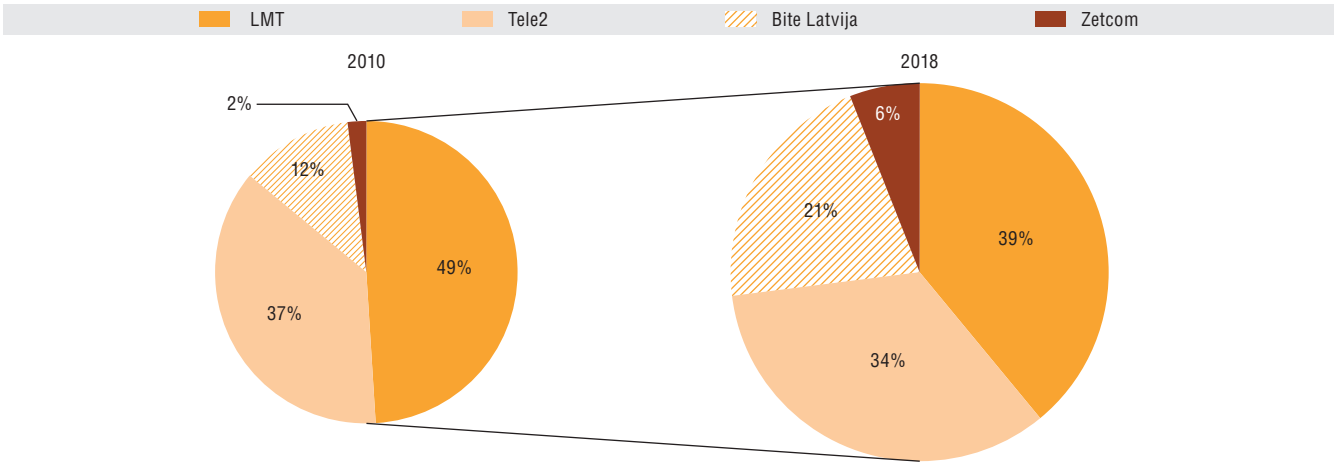
Mobile market developments

As of May 2020, there were three mobile network operators (MNOs) in Latvia: Latvijas Mobilais Telefons (LMT), Tele2 and Bite Latvija (Bite). Triatel, which offered CDMA services, exited the mobile market in 2020. All MNOs offer GSM/UMT/LTE services. In Latvia, 4G coverage is close to 100% of households and 4G is currently offered in parallel with 2G and 3G. As of mid-2019, there was no plan for operators to switch off their 2G and 3G networks in the near future.

Since 2010, the mobile market in Latvia has evolved and become less concentrated in comparison to December 2018. The largest MNO in terms of market shares since 2010 has been LMT, which experienced a reduction in market share from 49% to 39%, followed by Tele2 (increased from 37% to 34%) and Bite (grew from 12% to 21%) (Figure 3.17). However, Amigo, which is operated by Zetcom and the only mobile virtual network operator (MVNO) in the country, as well as being 100% owned by LMT, suspended its own operations and moved all customers to its host mobile network provider LMT, despite having experienced growth of mobile broadband subscriptions from 2% in 2010 to 6% in 2018.

Other positive developments in the Latvian mobile market include initiatives that may reduce the costs of network deployment by MNOs, such as network sharing. However, network sharing may also have effects on competitive dynamics in the market, which need to be closely monitored. In June 2019, for example, Tele2 and Bite signed a network sharing agreement for Latvia and Lithuania. The two operators' networks will form a joint shared network, which includes radio network and only excludes customer specific solutions. The partnership includes sharing of infrastructure for current networks, spectrum sharing and future 5G roll-out. This joint network will be deployed gradually starting in 2021, with the full network scheduled for completion by December 2023. Each party will hold 50% ownership in the joint venture (Tele2, 2019).

Figure 3.17. Mobile broadband market share in Latvia, 2010 and 2018

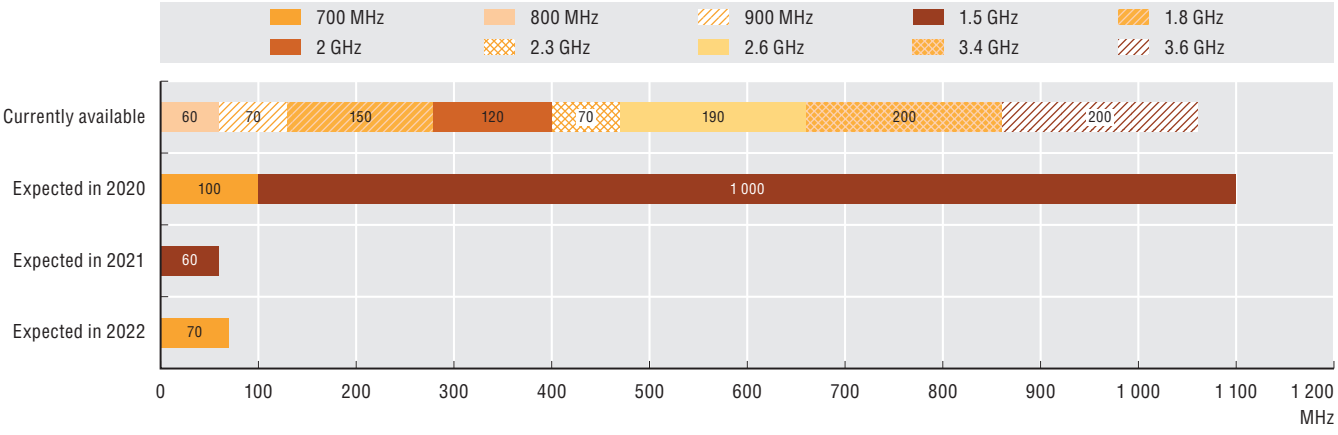


Source: SPRK (2018a), *Elektronisko sakaru nozares: faktos un skaitlos 2018* [Electronic communications sectors: facts and figures 2018], *https://infogram.com/id-es_nozares_raditaji_2018-1hxj48qk0y154vg?live.*

Spectrum allocation

One key resource and underlying condition of the mobile market is the availability of spectrum. Currently, the following frequency bands are assigned for wireless broadband in Latvia's national frequency plan: 450 MHz, 800 MHz, 900 MHz, 1.5 GHz, 1.8 GHz, 2 GHz, 2.3 GHz, 2.6 GHz, 3.4 GHz and 3.6 GHz (Figure 3.18). Despite advances in spectrum allocation, there is currently no secondary market for spectrum in Latvia. In addition to well-designed spectrum auctions, enabling a well-functioning secondary market could increase efficiency in the allocation of this scarce resource. Overall, five spectrum auctions have been held in Latvia since 2012 (Table 3.3).

Figure 3.18. Spectrum availability in Latvia, 2019



Note: As reported in December 2019.

Source: OECD, based on data from SPRK.

The 3.4-3.8 GHz band, which is suited for 5G deployment, is already fully assigned. Two mobile operators (LMT and Tele2) deployed the first 5G base stations in July 2019 in the 3.4-3.8 GHz band. The spectrum for wireless broadband services that remains to be assigned is mainly in the 700 MHz, 1.4-1.5 GHz and 26 GHz bands:

- The 700 MHz band is currently used for TV broadcasting (digital terrestrial television, DTT) by Tet, whose rights of use expire in 31 December 2021. The auction of the 700 MHz band is planned for the end of 2020 with commercial use from 2022 onwards.
- In January 2019, the use of the 1.4-1.5 GHz band (1427-1518 MHz) was allocated to communications services (European Commission, 2019). Assignment of the spectrum through an auction is planned for the end of 2020.

- Re-farming of the 26 GHz spectrum band is expected to be undertaken in 2020 with the auction anticipated for the end of 2020 or the beginning of 2021. While spectrum bands above 24 GHz are already used for 5G tests, realising the allocation of substantive frequency resources between 24.25 GHz and 27.5 GHz for 5G still requires co-ordination with the military (European Commission, 2019).
- Plans exist to make available 60 MHz of the 1.5 GHz bands in 2021, and around 80 MHz of the 700 MHz band in 2022 (a potential widening of available bands is under discussion).

Table 3.3. Spectrum auctions conducted in Latvia

Band	Year(s)	Proceeds (EUR million)	Auction result
791.0-821.0 MHz and 832.0-862.0 MHz	2013	4.7	Tele2, LMT and Bite
890.0-903.2 MHz and 935.0-948.2 MHz	1992	..	LMT
880.2-889.8 MHz and 925.2-934.8 MHz	2005	..	Bite
904.2-914.0 MHz and 949.2-959.0 MHz	2002	..	Tele2
903.3-904.1 MHz and 948.3-949.1 MHz	2008	..	Tele2
914-915 MHz and 959-960 MHz	2010	..	Tele2
1 710.0-1 734.8 MHz and 1 805.0-1 829.8 MHz	2001	..	LMT
1 735.2-1 759.8 MHz and 1 830.2-1 854.8 MHz	2000	..	Tele2
1 760-1785 MHz and 1 855-1 880 MHz	2005	..	Bite
1 920-1 940 MHz and 2 110-2 130 MHz; 1 960-1 980 MHz and 2 150-2 170 MHz	2002	..	LMT and Tele2
1 940-1 960 MHz and 2 130-2 150 MHz	2005	..	Bite
2 300-2 360MHz	2012	0.316	LMT and Bite
2 500-2 570 MHz and 2 620-2 690 MHz	2012	3.4	Four communications operators were granted rights of use from 1 January 2014 until 31 December 2028
2 570-2 620 MHz	2013	0.284	LMT
3 450-3 500 MHz, 3 600-3 650 MHz and 3 700-3 750 MHz	2002	..	Unistars (acquired in 2017 by Bite)
3 400-3 450 MHz and 3 650-3 700 MHz	2017	0.5	LMT
3 550-3 600 MHz	2018	6.53	Tele2

Notes: MHz = megahertz; .. = not available. Many spectrum blocks within the 900 MHz, 1.8 GHz and 2 GHz frequency bands were allocated and assigned by the Ministry of Transport (MoT) before the SPRK was established over different periods of time through the issuing of a licence, order or a decision. Some of the values on the fees paid on spectrum assignment previous to the establishment of SPRK are not available.

Source: SPRK (2018b), *Radiofrekvenču izsoles* [Radio frequency auctions], *www.sprk.gov.lv/content/radiofrekvencu-izsoles* (accessed on 6 May 2020).

In February 2002, the Cabinet of Ministers of Latvia approved the "Roadmap for the Deployment of Fifth generation (5G) Public Mobile electronic Communication Networks in Latvia". The document provides an overview of spectrum allocation, the deployment of commercial networks in large urban centres and coverage obligations for the allocation of 700 MHz related to railways and roads.

It should be noted that the national frequency plan of Latvia is technologically neutral with regard to frequency bands used for mobile communication services. As a result, operators can choose to deploy 5G using already assigned frequency bands if there are devices that allow them to do so. The results of the first 5G tests were shown during a regional conference – 5G Techritory, the 1st Baltic Sea Region 5G Ecosystem Forum – which took place in Riga in September 2018 (5G Techritory, 2019; European Commission, 2019).

In the same month, Estonia, Latvia and Lithuania signed a Memorandum of Understanding (MoU), agreeing to co-operate on the deployment of the 4G+, 4G ++ and 5G network along a section of the Via Baltica covering Tallinn, Riga and Kaunas (in Lithuania), in order to foster innovation in transportation systems and test autonomous vehicles (The Baltic Course, 2018). In November 2019, this MoU, now including Poland, evolved into a joint roadmap to establish a common approach to map existing infrastructure and determine funding gaps for infrastructure deployment and shared principles for infrastructure deployment along the Via Baltica.

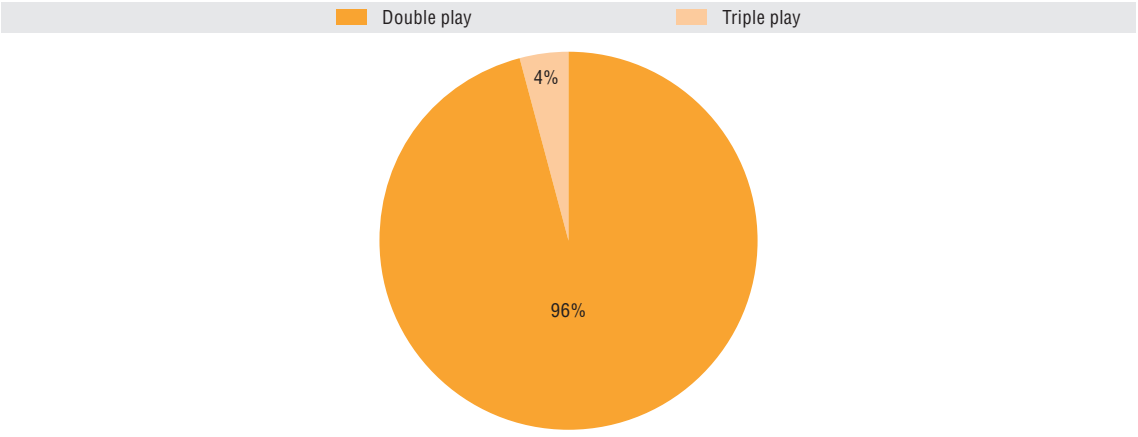
In order to foster 5G, the MoT is working on two pilot projects to deploy 5G-enabled passive infrastructure along both the Via Baltica and Rail Baltic routes, pending available funds. Measures to reduce deployment costs and administrative burdens through a lighter regime for small cell deployment, and to ease access to information on financial support mechanisms from the European Union, are also being envisioned.

Convergence

Trends related to the offer of bundled services, as well as the offering of audio-visual content through IP networks, are of particular importance, since bundles function as an indicator of the degree of convergence in consumer offers.

At present, the bundled services market in Latvia is characterised mainly by double-play offers: 96% of sold bundles are double-play bundles, with triple play accounting for only a small fraction of offers (4%) (Figure 3.19). Due to the absence of vertically integrated players in Latvia, there are currently no quadruple-play offers. The fixed incumbent, Tet, does not have a mobile operation and, in April 2016, the option of a merger between the fixed incumbent and the mobile incumbent (LMT) was rejected by the government (which owns 51% of Tet). Since then, the Telia Group (which holds 49% of Tet) changed its global governance and merged its fixed and mobile affiliates in Estonia, which could affect future merger discussions in Latvia (European Commission, 2019; Telecompaper, 2019).

Figure 3.19 Customers subscribing to bundled services in Latvia, 2018



Note: Double play can be voice + Internet, TV + Internet or voice + TV; triple play is voice + Internet + TV.
Source: OECD, based on data from SPRK.

SPRK has not defined a relevant market for bundled services. However, the impact of bundling practices on competition dynamics is perceived as positive, since infrastructure-based competition exists in Latvia and alternative operators are able to replicate the offers of the incumbent Tet.

Mobile operators are competing with the fixed incumbent through fixed-wireless offers by offering TV and Internet services using dedicated 4G routers at home. However, a study by SPRK concluded that mobile broadband cannot yet be considered a full substitute for fixed broadband in Latvia (European Commission, 2019). Nevertheless, unlimited mobile broadband services, including dedicated broadband services using 4G routers at home, may become a partial substitute in the future once mobile networks are further upgraded. Meanwhile, a convergence between fixed and mobile networks can be observed at the core of the networks through the deployment of fibre deeper into fixed, but increasingly also mobile networks, to meet the increasing demands of the digital transformation. For example, in 2017 about 54% of mobile cellular traffic around the world was offloaded to fixed networks through Wi-Fi or small, low-power cellular base stations (CISCO, 2018). In a way, wireless networks become extensions of fixed networks, and as the demand for mobile data traffic increases, wireless networks rely increasingly on fixed broadband infrastructure. This trend will continue and deepen with 5G networks.

In terms of provision of audio-visual services over IP networks, there are several IPTV offers in Latvia. IPTV providers have been authorised as communication providers and follow the same rules as operators who provide traditional pay TV or any other communication service (OECD, 2019b).

Another category for the provision of audio-visual content over IP networks is over-the-top (OTT) services, which may be provided by online companies or communication providers (e.g. Shortcut OTT provided by Tet). Currently, OTTs do not require an authorisation from the SPRK and do not need to meet quality of service (QoS) obligations. However, discussions are underway regarding treatment of this category in the context of the transposition of the new regulatory framework.

Interestingly, the Latvian telecommunication sector has also seen convergence trends with other utilities and services sectors. In 2017, following the liberalisation of electricity sector, the communication incumbent Tet entered the electricity market as a reseller, offering bundles with communication services. Tet also sells phones, TV sets, computers, drones and other equipment; offers smart home solutions; and provides data centres, cloud services, entertainment, different IT services, as well as different marketing tools. The incumbent also offers e-learning solutions for senior adults.

Finally, the mobile operator Bite also provides travel insurance, insurance for the screens of tablets and phones, and antivirus protection. LMT, in collaboration with Riga Technical University, is developing artificial intelligence (AI) solutions to provide rescue solutions with the help of drones in the event of forest fires and missing people.

Regulatory and policy developments in Latvia

Institutional framework and design

There are several authorities involved in communication markets in Latvia, some of which have regulatory functions, while others are responsible for policy formulation (e.g. broadband development policies).

The authority responsible for developing broadband policies is the Ministry of Transport (Satiksmes Ministrija). Among other responsibilities, the Ministry of Environmental Protection and Regional Development (Vides Aizsardzības un Reģionālās Attīstības Ministrija, VARAM) is responsible for the development of national frequency and numbering plans. The Public Utilities Commission (Sabiedrisko Pakalpojumu Regulēšanas Komisija, SPRK) is responsible for the regulation and supervision of the communication sector, and the National Electronic Mass Media Council (Nacionālā Elektronisko Plašsaziņas Līdzekļu Padome, NEPLP) is responsible for the regulation and supervision of the audio-visual sector. The Competition Council (Konkurences Padome) functions as the competition authority for all sectors.

Ministry of Transport

The MoT is responsible for implementing public policy in the fields of transport and communication. The Ministry has a broad mandate; however, only a limited number of staff are responsible for dealing with communication issues. The MoT co-operates with SPRK on issues related to broadband policy planning, recent developments and trends in the sector, frequency planning and the transposition of the European Union Directives into national legislation.

Ministry of Environment Protection and Regional Development

In addition to its digital government and strategy role, the Ministry of Environment Protection and Regional Development (VARAM) is responsible for the policy-level development of national frequency and numbering plans. The technical aspect of spectrum and numbering management, however, has been delegated to the Electronic Communications Office of Latvia (ECO) (VAS Elektroniskie Sakari, VASES), which is 100% state-owned. ECO was established under the MoT in 2004 and re-structured under VARAM in 2011, following a recommendation of the European Commission that considered the presence of LVRTC, the state-owned operator, and the technical role of spectrum management under the same ministry, to be problematic.

Two permanent working groups on frequencies and numbering issues exist to provide inter-institutional co-ordination. ECO is responsible for carrying out surveys with operators and consulting with other institutions, in co-ordination with VARAM and SPRK. ECO is also responsible for co-ordinating the

allocation of frequencies in accordance with international treaties, in co-operation with SPRK. ECO collects the fees for spectrum usage (following the Directive from the European Commission 2002/20) and uses the revenues to fund its operating costs, which include monitoring harmful interference.

Public Utilities Commission

The Public Utilities Commission (SPRK) is an independent multi-sectoral regulatory authority established in 2001, with regulatory responsibilities for the following sectors: communication services, energy, postal services, waste disposal and water management. The Law on Regulators of Public Utilities is the primary legislation governing its functions. Its aim is to ensure "the possibility of receiving continuous, safe and qualitative public utilities whose tariffs conform to economically substantiated costs, as well as to promote development and economically substantiated competition in regulated sectors" (SPRK, 2019). According to an OECD (2016) peer review of SPRK, the current multi-sector setup of SPRK is a distinguishing feature that allows the regulatory process – related specifically to tariffs, setting methodologies and registration of utilities – to be applied across the regulated sectors.

The *Regulations Regarding Types of Regulated Public Utilities* (Republic of Latvia, 2009) state that the distribution services of radio or television programmes in public communication networks shall be regulated and that, according to national legislation, SPRK is the responsible entity. SPRK, thus, is responsible for broadcasting related to signal transmission and broadcasting networks, but not the content or operations of mass media. The National Electronic Mass Media Council (NEPLP) supervises the compliance of operations of the electronic mass media. The role of both authorities does not overlap.

As mentioned above, the mandate of VARAM involves managing frequency and numbering planning, which is carried out through ECO in co-operation with SPRK.

National Electronic Mass Media Council

The NEPLP is an independent, autonomous institution that supervises the regulatory compliance of mass media operations in Latvia. The Council is responsible for issuing broadcasting and retransmission permits, authorising pay TV service providers and monitoring developments in the audio-visual sector in Latvia.

Policy and regulatory initiatives to enhance access

This section discusses policy and regulatory initiatives such as those aiming to reduce deployment costs, streamline administrative procedures and enhance access to resources by operators. It also assesses programmes to foster access and use of communication services and expand high-speed fixed broadband infrastructure in rural and remote areas.

Expanding access

In Latvia, the main programme for expanding access in rural and remote areas is the state aid programme "Next Generation Network for Rural Areas" (2012-2020), co-financed by the European Regional Development Fund (ERDF). The programme was established to improve the availability of communication networks in rural areas, by ensuring the deployment of middle-mile backbone infrastructure in areas where no service provider had infrastructure or had no plans to deploy fast broadband of at least 30 Mbps within the following three years. Within the framework of the rural broadband programme, the Latvia State Radio and Television Centre (Latvijas Valsts Radio un Televīzijas Centrs, LVRTC), the state-owned operator, is responsible for building an open access middle-mile infrastructure in identified "white areas", to which retail providers have wholesale access. The total funding made available for the rural broadband programme was EUR 72.7 million.

During the planning stage of the programme, an analysis requested by MoT was carried out in 2011 to evaluate stakeholder satisfaction regarding broadband speeds within municipalities in areas with low population density, and expectations of demand growth for broadband networks and services. On the basis of this analysis, a draft list of white areas was published and put forth for public consultation before approval by the Optical Network Monitoring Committee.

Project implementation was divided into two stages. The first stage, completed in August 2015, aimed to deploy 177 access points and 1 813 km of fibre, while enabling operators to connect to the network at any location along the route. LVRTC achieved all the objectives of the first phase.

Another analysis was conducted in 2014 to update the list of areas due to benefit from the rural broadband programme and to determine which areas most interested service providers. The findings identified a further 221 white areas in Latvia. The second stage, starting in 2015 and due to be finished by December 2021, was therefore designed with the objective of deploying a further 220 access points and 2 000 km of fibre. LVRTC signed contracts amounting to EUR 40.7 million for the deployment of a total of 1 950.6 km of the planned 2 000 km.

As of January 2019, 1 234 km of fibre and middle-mile service were available in 73 out of 220 access points in white areas. However, the interest of service providers, including mobile network operators, has been lower than initially expected. As of January 2019, LVRTC had signed leases for 78 rented sections with a total length of 1 648.3 km of fibre. Currently, the network is used by only 12 operators and the largest client is the fixed incumbent Tet. Out of the total fibre deployed in rural areas, around 930 km are leased to Tet, which provides fixed broadband services to end users.

Overall, the rural broadband project represents a positive step towards closing the digital divide in Latvia. A key challenge, however, is the dependence on last-mile infrastructure set up by operators. In order to fully benefit from the programme, the next phase should focus on ways to better provide last-mile connectivity. Approaches could include supply-side measures, including an analysis to identify ways to further reduce deployment costs and streamline administrative procedures for last-mile deployment, and demand-side measures aiming at driving broadband demand by individuals and businesses (in particular small and medium enterprises), as well as educational institutions, as currently planned through a partnership between the MoT and the Ministry of Education (Box 3.1).

Box 3.1. Broadband for schools in Latvia

The Ministry of Transport (MoT) plans to attract additional resources (2020-23) for broadband deployment and expansion of access points in educational institutions, in order to respond to the growing demand for connectivity in schools, assist with implementation of the new curriculum by the Ministry of Education and enable distance learning.

A survey conducted by the Latvian Municipal Union found that broadband infrastructure from the "Next Generation Network for Rural Areas" programme was available in the vicinity of around 70 educational institutions. Following these results, LVRTC conducted an initial assessment and found that, under the current rural programme, middle-mile connectivity could be deployed to 17 education institutions located in white areas. The amendment to the project was then expanded to accommodate 21 access points in educational institutions. However, even when approved, the project will not cover all educational institutions in the country. In April 2020, the MoT launched a procurement process to identify the actual needs of remaining educational institutions.

In addition to the rural broadband programme, Latvia has also put in place a universal service obligation (USO) which provides discounts for voice telephony and broadband services to people with disabilities. As of 2018, 3 790 users benefited from the USO reductions. Potential revisions of this obligation will be discussed in the context of the revision of Latvia's Electronic Communications Law, intended to transpose the provisions of the European Electronic Communications Code. The scope of the USO may change starting in 2022 and could include a minimum QoS level for broadband access to support applications requiring higher speeds. However, further efforts could be undertaken to reduce deployment costs for operators. In addition, supply-side measures could be complemented by demand-side measures.

Competition

SPRK co-operates closely with the Competition Council, with both bodies sharing information required to perform their tasks. SPRK gives the Competition Council the opportunity to comment on all draft market analyses (e.g. in the context of termination, local loop unbundling bitstream access, leased lines and others) based on the EU regulatory framework prior to its adoption. None of SPRK's decisions were appealed in 2018.

In Latvia, barriers to competition have historically been related to barriers to entry and network expansion, and are used by SPRK as relevant criteria to measure the market power of operators in Latvia. Barriers can differ in different markets (e.g. voice, broadband, leased lines, termination markets etc.).

Following liberalisation, barriers to entry, expansion and competition were very high, especially regarding network deployment. Over the years, competition and innovative solutions, as well as the capacity to adapt to the rapidly changing communication market, has enabled mobile and fixed operators to overcome some of those barriers, and deploy and maintain high-quality networks. The principle of technological neutrality applied by SPRK and the creation of proportionate circumstances for operators have been crucial to promoting competition.

The market entry of Bite in 2005 increased competition in the mobile voice market. Regulations in the areas of termination rates and portability further contributed to increased competition and, in turn, to enhanced quality of service and lower prices for consumers.

In 2018, SPRK conducted a market analysis and found that mobile voice could be considered a substitute for fixed voice. Given the assessment that competition in the voice market was effective, retail and wholesale voice markets were deregulated (with the exception of termination rates). As of mid-2019, only 3.5% of all voice traffic relates to fixed voice. Termination rates continue to be regulated in Latvia, given the characteristics of the wholesale voice call termination markets, which led to the conclusion that barriers to entry remain high in this market segment.

An issue raised by some industry players in the context of voice telephony, however, relates to the offers of certain operators that include unlimited calls to only a number of networks. One example is Bite's consumer offer. The offer for some tariff plans includes unlimited calls to Bite, LMT, Tele2 and Tet networks, but not to smaller fixed networks. Following SPRK decision No. 1/19 of January 2018 ("Regulations on notification of end users about premium rate calls"), customers receive a verbal notification whenever calls go to numbers not from the above-mentioned four largest communication providers in Latvia (three mobile providers and the incumbent Tet for fixed services). The issue may warrant detailed analysis by Latvian entities with respect to potential competition effects on certain networks in the country.

In terms of broadband services, SPRK found that mobile broadband services cannot yet be considered as full substitutes for fixed broadband services in Latvia, while recognising that fixed broadband operators face competition to some extent from mobile operators. It has been determined that the incumbent Tet has had significant market power (SMP) in the wholesale broadband access markets since 2007. Although barriers to entry are considered to be high, some alternative operators have deployed their own infrastructures in more densely populated areas in Latvia. Having analysed the competitive conditions against a set of criteria, SPRK concluded that the market cannot yet be considered effectively competitive and that regulation is still warranted.

The wholesale high-quality market, comprising leased lines, virtual private networks and high-quality broadband with guaranteed bandwidth used by business customers, itself is comparatively small in Latvia. Moreover, the number of leased lines and revenues has decreased significantly over the years. SPRK identified a trend reflecting migration from leased lines and VPNs (implemented and managed by network operators) to Internet connection with usage of cloud services or self-deployed software-based VPNs. Existing competition conditions, where not only Tet is present but also alternative operators, and the changing dynamics of the market, suggested the presence of effective competition and indicated that regulation was no longer necessary. Accordingly, SPRK deregulated the wholesale high-quality market in December 2019.

Wholesale regulation and infrastructure sharing

Termination rates are regulated in Latvia. Reductions in wholesale termination rates have resulted in positive implications for end-user prices as well as greater availability of number portability. Historically, termination rates have been considered too high in Latvia and a hindrance to new entrants. In order to avoid abuse, the list of SMP operators in Latvia is frequently updated and both Fixed Termination Rates (FTRs) and Mobile Termination Rates (MTRs) have been regulated (the maximum FTR was set at EUR 0.000701/minute and the maximum MTR at EUR 0.008868/minute in January 2018) (European Commission, 2019).

In Latvia, the most significant development in terms of wholesale regulation has been asymmetrical, applied to the ducts and poles of the incumbent Tet (designated as having SMP in several markets), and mandated in 2014 by SPRK. Historically, Tet has been regulated with respect to retail voice, leased lines, wholesale voice origination, transit, wholesale broadband access and wholesale leased lines. The majority of these markets have been gradually deregulated. Tet is currently regulated only in the context of unbundling and bitstream access including access to ducts and poles. Moreover, wholesale terminating segments of leased lines are soon to be deregulated.

While these SMP remedies do not include access to cables, SPRK has adopted other remedies such as local loop unbundling and wholesale bitstream access, so that other operators with limited coverage can use the network of Tet and compete at the retail level. Furthermore, Tet is subject to rules including non-discrimination, transparency, price control, cost accounting and accounting separation (European Commission, 2019).

In urban areas of Latvia, such as Riga, competition continues to be infrastructure-based, through the deployment of aerial cables from roof to roof (European Commission, 2019). However, this typically does not comply with regulations requiring the underground installation of cables to offer a safe, protected and hidden environment for communication networks. Urban guidelines and regulations of municipalities around the country, such as those in Riga, prohibit over-head cables in historical areas. Moreover, even though local loop and bitstream access have not been found to be widely used (since operators in densely populated areas compete with their own infrastructures), the SMP remedies lower barriers to expanding broadband service offers mainly at the retail level and, where feasible, promote service-based competition.

In 2017, the European Commission's Broadband Cost Reduction Directive (BCRD) was fully transposed on to national legislation. The Law on High-Speed Electronic Communications foresees mandatory provision of access to physical infrastructure (e.g. pipe, mast, duct, inspection chamber, manhole, cabinet, building or entry to a building, antenna installation, tower and pole) to operators authorised to provide communication services, as well as other utility providers (e.g. gas, electricity, heating, transport and sewage services). Such access should be provided under fair and reasonable terms and conditions, including the price, in order to deploy high-speed networks. SPRK is the Dispute Settlement Body (DSB) designated by the Directive.

While there is no mapping obligation, in order to improve co-ordination and bridge information gaps, communication operators can access a data portal for a fixed fee, through the Single Information Point of Latvia (*www.latvija.lv*). This portal includes existing information collected by the government on the physical infrastructure of any network operator (i.e. location, route, type, current use of the infrastructure and contact point). In the event of any missing information, access seekers can request data from the infrastructure owners or through a visit to the physical infrastructure. The 2017 law also foresees the co-ordination of civil works, mandating that communication providers and other infrastructure providers must co-ordinate to effectively deploy high-speed networks.

In order to avoid two-layer regulation, during the process of transposition of the BCRD, the provisions in the 2017 law were linked to provisions under the Electronic Communications Law of 2014, which regulates symmetrical access. Six operators (including Tet) currently provide access to their duct system to other operators. However, operators potentially interested in accessing the infrastructure of the incumbent claim that, in reality, they are refused access on the basis of insufficient capacity, due to the future capacity needs of the incumbent. Operators are also required to pay a fee each time they request an assessment of available capacity. Poles in rural areas, in particular, have not been used for these and other reasons, despite the evident interest in infrastructure sharing.

With regard to other utilities, companies providing energy (Latvenergo), railway (Latvijas Dzelzceļš), water, sewerage and gas services also have communication needs and have been installing fibre and upgrading their infrastructure (i.e. to support control systems, smart metering, signalling, rail track, safety management, etc.).

Some existing fibre installation projects using the infrastructures of other utilities in Latvia were negotiated based on mutual interest before the transposition of the BCRD. These include a collaboration between Latvenergo and Tet, established in 1994, which covers underground fibre cable installation and optical fibre ground wire (OPGW) cable technology in high-voltage aerial power lines. Due to safety standards, high-voltage aerial power lines must have lightning protection wire (i.e. shield wires) installed above power lines (mostly 110 kV), which were historically made of steel. These have been gradually replaced by OPGW cables, which provide grounding and communication capabilities, in addition to being more resistant (being surrounded by layers of steel and aluminium wire). Latvenergo and Tet have jointly deployed 1 847 km of OPGW cables and underground fibre under an arrangement where some fibre strands are allocated to Latvenergo and some to the core network of Tet.

In order to reduce deployment costs (including those concerning rights of way), a number of operators have capitalised on opportunities to deploy fibre networks along roads and railways. In 2019, seven operators in Latvia used the infrastructure along roads, and four operators used the infrastructure of Latvijas Dzelzceļš to install fibre along railways or used towers for mobile operators to install base stations. Operators in Latvia also make use of shared access to towers and masts. All mobile network operators provide access to their masts and five fixed operators provide access to their masts and towers.

Although infrastructure-sharing cases for the deployment of backhaul exist, infrastructure sharing in Latvia is still limited, particularly concerning the use of infrastructure of other utilities. Following the guidance of the BCRD, the 2017 Law on High-Speed Electronic Communications Network mandates that "upon receipt of a permit to build a new or re-build an existing residential house or non-residential building, the initiator of the construction shall ensure that the internal physical infrastructure is suitable for the high-speed electronic communications network" (Republic of Latvia, 2017). However, the law also provides some exceptions, notably, if there is already suitable infrastructure, if there are objective reasons for the failure of ensuring suitable infrastructure or if the intended use of the building does not require the use of high-speed networks.

However, certain existing multi-dwelling buildings in Latvia (under a specific form of ownership rare in other European countries, where each owner of the flat has partial ownership of shared premises of the building such as a stairway, basement, etc.) were excluded from this obligation in the 2017 law, on the basis that such an obligation would breach constitutional property rights. The extent to which these residencies constitute a substantial proportion of the buildings without suitable infrastructure for high-speed broadband remains to be assessed.

The measures foreseen in the BCRD fall under the purview of the MoT. Exceptions concern the Dispute Settlement Body (DSB), the functions of which are fulfilled by SPRK. No disputes have occurred in relation to application of the Directive.

Consumer protection

SPRK co-operates with the Authority for Consumer Rights Protection (PTAC) in order to protect consumer rights in the regulated sectors. SPRK's responsibilities concern terms of contracts, tariffs and QoS for communication services. PTAC's mandate relates to the application of contract rules. Up to November 2018, SPRK had received and replied to 45 consumer complaints regarding QoS (16%), tariffs (16%), bills (18%), terms of contracts (24%) and other (27%) non-competency cases. PTAC received 93 individual complaints on communications providers (European Commission, 2019).

SPRK supervises the compliance of operators regarding specific quality requirements and publishes the results of mobile broadband quality measurements. It performs two types of Internet quality measurements – serial measurements and sample measurements. Serial measurements are performed in specific locations over a full 24-hour day for at least one week. They provide an overview of mobile Internet performance during the day and show changes in Internet speed at different times. Sample

measurements are performed in different geographical locations throughout Latvia and give an overview of actual mobile Internet quality indicators. This tool has been especially useful for consumers to compare the quality of mobile broadband services of all mobile operators in different geographical areas. Moreover, an independent tariff comparison tool has been available online for several years (*www.gudriem.lv*).

In relation to advertisement practices of fixed broadband services in Latvia, the maximum (advertised) speed must be the average speed that the end user receives constantly during the day (except for peak hours), and the minimum guaranteed speed must be at least 20% of the maximum speed or the upper limit of a maximum speed range indicated in a contract. For mobile services, the minimum guaranteed speed must be at least the lower limit of a broadband connection speed (i.e. 256 kbit/s). SPRK also mandates that ISPs include maximum speeds within contracts.

SPRK quality measurements performed by SPRK are a useful tool to promote competition and encourage upgrades of mobile networks, since the results are publicly available. They also allow operators to monitor the performance of their networks. In Latvia, the number of consumer complaints regarding QoS are low, amounting to 7 out of 45 consumer complaints, as of November 2018. However, no specific consumer satisfaction survey on QoS has been conducted to date (European Commission, 2019).

Network neutrality

In Latvia, network neutrality rules are being implemented in accordance with European Union Regulation 2015/2120. In order to monitor compliance, SPRK requests information from ISPs, analyses end-user complaints, performs technical measurements (constantly for mobile networks and only in the event of complaints in fixed networks) and checks information on ISP webpages.

Regarding network neutrality issues, no breach of European Union regulation has been identified (European Commission, 2019). The main areas of SPRK with respect to network neutrality are: transparency (contract information), Internet speeds, monitoring mechanisms (to test non-conformity of performance) and traffic management (including port-blocking).

SPRK reported that in 2018, 19% of ISPs had been carrying out traffic management measures (i.e. to prevent malware, malicious applications and spam) (European Commission, 2019). One mobile operator (Bite) provides zero-rated offers. Applications such as social media, voice, short message service and geographical navigation service applications are zero-rated. Due to the lack of complaints regarding zero-rating practices, as well as the broad availability of subscriptions with unlimited Internet and competitive prices among all Latvian mobile operators, SPRK did not consider the zero-rated offers provided by Bite to be harmful. Moreover, as Bite is the smallest mobile operator in Latvia, its zero-rated offer is considered as an attempt to attract new customers and a tool to foster competition.

Policy recommendations

Overall, Latvia is performing well regarding the deployment of both fixed and mobile broadband high-speed networks. Nonetheless, a few weaknesses persist in the policy design and regulatory framework which may hinder efforts to bridge the digital divide, the efficient allocation of spectrum for wireless services, adoption of the IoT, the deployment of IPv6, attempts to foster convergence and preparation for emerging technologies (e.g. 5G).

- **Institutions**. Latvia would benefit from a holistic policy and regulatory approach towards connectivity. Consideration could be given to the creation of a converged regulator dealing with communication, broadcasting and media services. Currently, functions are divided between SPRK and the NEPLP. Developments in convergence over IP networks and potential convergence between fixed and mobile networks have and will increasingly effect market structures. A converged regulatory structure would enable those changes to be more efficiently addressed taking into account overarching challenges and trends. At the ministerial level, while roles are currently shared between the MoT and VARAM, the institutional design could benefit from the establishment of one clear focal point. Finally, limitations on hiring public sector staff, including experts with communication expertise, can hinder policy making and the acquisition of technical knowledge within institutions.
- **Civil works and rights of way**. The territory planning of municipalities could be improved by promoting dig-once policies, permitting new towers, planning new routes for fibre and grounding cables,

harmonising procedures (e.g. registration of network sites) and simplifying administrative processes for network deployment. Municipalities could also co-ordinate among each other and with the MoT to promote platforms where service providers can consult available sites to deploy base stations (e.g. rooftops of government buildings). Bottlenecks in fixed and mobile network deployment at the level of municipalities will become more pronounced with network densification as a result of 5G deployment. In addition, access to infrastructure will be crucial to install the large number of antennas required for 5G.

- **Infrastructure access and sharing**. Efforts should be made to reduce information asymmetries concerning available infrastructure and monitor potentially discriminatory practices concerning access to passive infrastructure, particularly by companies with significant market power.
- **Competition**. Despite positive developments in the mobile market, competition concerns still exist in the fixed broadband market in Latvia, with one company having a 56% market share. Monitoring of this situation should continue and should include implementation of infrastructure-sharing obligations.
- **Last-mile access**. Bridging the connectivity gap in isolated, less economically attractive areas will be the main infrastructure challenge going forward. The next phase of the rural broadband programme in Latvia should focus on last-mile solutions to close connectivity gaps. Measures could focus on further reducing deployment costs and streamlining administrative procedures, as well as fostering demand-side measures to drive demand by individuals, businesses (in particular, small and medium enterprises) and educational institutions.
- **Spectrum**. While Latvia is well advanced in terms of frequency allocation, there is currently no secondary market for spectrum. Updating the regulatory framework to allow such markets would enable more efficient use of spectrum.
- **IoT**. The IoT holds promise to increase innovation and efficiency in multiple sectors, such as energy or industry automation. However, Latvia is lagging behind in M2M and IoT take-up. While a new numbering plan is being considered respond to the needs of M2M and IoT, no broader plan exists to identify challenges and foster these services. Operators have also expressed concerns regarding the lack of demand from businesses and consumers for these services. Latvia should establish a broader IoT plan to identify existing challenges and foster a broader IoT ecosystem and adoption of IoT services in the country.
- **IPv6**. Latvia is lagging behind regarding adoption of IPv6. IPv6 is not only important because of the scalability of future Internet developments, but also crucial from a security perspective as IPv6 may be more conducive to end-to-end encryption. The latter factor may be favourable to the security of industrial IoT applications, among others. While Latvia has put in places measures to increase IPv6 adoption in the public sector, the implementation of a thorough IPv6 strategy is recommended, in order to foster ample deployment. This should be performed in co-ordination with civil society, the private sector and technical stakeholders, as was done in Sweden.
- **IXP**. Some of Latvia's Internet exchange points have only a limited number of participants. The design of the Latvian Internet exchange point LIX, in particular, hinders its potential for further growth, due to traffic limitation to Latvian prefixes. The regulator or ministry (either VARAM or MoT) should work with existing IXPs and networks in the country to improve the management and performance of IXPs based on international good practices, in order to increase the amount of traffic exchanged locally. An analysis of the state of traffic exchange in the country and the performance of existing IXPs could serve as a starting point for such an undertaking.

Box 3.2. Policy recommendations

To ensure that Latvia is prepared for forthcoming developments in communication technologies and markets, the government should:

- evaluate the benefits of creating a converged regulator for both communication and broadcasting services, particularly in relation to increasing convergence of services over IP networks
- establish a clear ministerial focal point for communication services, as competencies are currently dispersed between the Ministry of Transport (MoT) and the Ministry of Transport and the Ministry of Environmental Protection and Regional Development (VARAM)

Box 3.2. Policy recommendations *(cont.)*

- improve territorial planning in municipalities by promoting dig-once policies, granting permission for new towers, and planning new routes for fibre and cables, as well as harmonising and simplifying administrative procedures for network deployment
- increase co-ordination among municipalities and the MoT to overcome bottlenecks on fixed and mobile network deployment, and to prepare for network densification required by 5G
- reduce information asymmetries regarding available infrastructure and closely monitor the situation for potentially discriminatory practices regarding access to passive infrastructure
- monitor the state of competition in the fixed broadband market and implement infrastructure-sharing obligations as appropriate
- engage local stakeholders in the rural broadband programme on last-mile solutions and foster demand through targeted initiatives
- update the regulatory framework to allow for a secondary spectrum market to promote more efficient use
- develop and implement a national IoT plan to identify challenges and foster demand from businesses and consumers
- develop and implement a comprehensive IPv6 strategy in co-ordination with civil society, the private sector and technical stakeholders
- carry out an analysis of the state of traffic exchange and promote the deployment of neutral IXPs, based on good international practices, in order to improve traffic exchange and foster a well-functioning Internet ecosystem.

References

5G Techritory (2019), *5G Techritory*, *www.5gtechritory.com/story* (accessed on 9 November 2019).

Akamai (2020), "IPv6 adoption visualization", *www.akamai.com/uk/en/our-thinking/state-of-the-internet-report/state-of-the-internet-ipv6-adoption-visualization.jsp* (accessed in June 2020).

APNIC (2020), "IPv6 measurement maps", *http://stats.labs.apnic.net/ipv6* (accessed in June 2020).

CISCO (2018), *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017–2022 White Paper,* Cisco Systems, San Jose, CA, *www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.html* (accessed on 20 September 2019).

CRCT (2019), *Communications Monitoring Report 2019*, Canadian Radio-television and Telecommunications Commission, Ottawa, *https://crtc.gc.ca/eng/publications/reports/policymonitoring/2019/index.htm*.

European Commission (2019), *DESI Report 2019 – Telecommunication Chapter of Latvia*, European Commission, Brussels, *https://ec.europa.eu/digital-single-market/en/news/2019-desi-report-electronic-communications-markets-overview-member-state-telecom-chapters*.

European Commission (2018a), *Study on Broadband Coverage in Europe 2018*, Brussels, *https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62760*.

European Commission (2018b), *DESI Report 2018 – Telecommunication Chapter of Latvia*, Brussels, *https://ec.europa.eu/digital-single-market/en/scoreboard/latvia*.

European Commission (2016), *Connectivity for a Competitive Digital Single Market – Towards a European Gigabit*, Brussels, *https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=17182*.

European Commission (2010), *Digital Agenda for Europe*, Brussels, *https://ec.europa.eu/digital-single-market/en/digital-agenda-europe-key-publications*.

FCC (2019), *2019 Broadband Deployment Report*, Washington, DC, *www.fcc.gov/reports-research/reports/broadband-progress-reports/2019-broadband-deployment-report*.

Google (2020), "Per-country IPv6 adoption", *www.google.com/intl/en/ipv6* (accessed in June 2020).

M-Lab (2019), "Worldwide broadband speed league", *www.cable.co.uk/broadband/speed/worldwide-speed-league* (accessed on 9 May 2020).

OECD (2020a), *OECD Telecommunications and Internet Statistics* (database), *https://doi.org/10.1787/data-00170-en* (accessed on 9 July 2020).

OECD (2020b), *OECD Broadband Portal* (database), *www.oecd.org/sti/broadband/oecdbroadbandportal.htm* (accessed on 6 May 2020).

OECD (2019a), *Measuring the Digital Transformation: A Roadmap for the Future*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264311992-en*.

OECD (2019b), "The road to 5G networks: Experience to date and future developments", *OECD Digital Economy Papers*, No. 284, OECD Publishing, Paris, *https://dx.doi.org/10.1787/2f880843-en*.

OECD (2018a), "Bridging the rural digital divide", *OECD Digital Economy Papers*, No. 265, OECD Publishing, Paris, *https://dx.doi.org/10.1787/852bd3b9-en*.

OECD (2018b), *OECD Reviews of Digital Transformation: Going Digital in Sweden*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264302259-en*.

OECD (2016), "Driving performance at Latvia's Public Utilities Commission", *The Governance of Regulators*, OECD Publishing, Paris, *http://dx.doi.org/10.1787/9789264257962-en*.

OECD (2014), "The Internet in transition: The state of the transition to IPv6 in today's Internet and measures to support the continued use of IPv4", *OECD Digital Economy Papers*, No. 234, OECD Publishing, Paris, *https://dx.doi.org/10.1787/5jz5sq5d7cq2-en*.

Ookla (2019), "Speedtest", *www.speedtest.net/global-index* (accessed on 9 May 2020).

Republic of Latvia (2017), *Law on High-speed Electronic Communications Network*, Likumi, Riga, *https://likumi.lv/ta/en/en/id/289933-law-on-high-speed-electronic-communications-network*.

Republic of Latvia (2009), *Regulations Regarding Types of Regulated Public Utilities of 27 October 2009*, Riga, *www.vvc.gov.lv/export/sites/default/docs/LRTA/MK_Noteikumi/Cab._Reg._No._1227_-_Regarding_Types_of_Regulated_Public_Utilities.doc*.

SPRK (2019), *Mission, Objective and Functions*, Public Utilities Commission, Riga, *www.sprk.gov.lv/en/content/mission-objective-and-functions* (accessed on 12 December 2019).

SPRK (2018a), *Elektronisko sakaru nozares: faktos un skaitlos 2018* [Electronic communications sectors: facts and figures 2018], Public Utilities Commission, Riga, *https://infogram.com/id-es_nozares_raditaji_2018-1hxj48qk0y154vg?live*.

SPRK (2018b), *Radiofrekvenču izsoles* [Radio frequency auctions], Public Utilities Commission, Riga, *www.sprk.gov.lv/content/radiofrekvencu-izsoles* (accessed on 6 May 2020).

Steam (2019), "Steam download stats", *https://store.steampowered.com/stats/content* (accessed on 9 May 2020).

Tele2 (2019), "Tele2 and Bite sign agreement to share networks in Latvia and Lithuania", *Tele2*, *www.tele2.com/media/press-releases/2019/tele2-and-bite-sign-agreement-to-share-networks-in-latvia-and-lithuania#:~:text=Tele2%20and%20Bite%20have%20today,the%20upcoming%205G%20roll%2Dout*.

Telecompaper (2019), "Telia to re-assess position in Latvia after cooperation with govt stalls", *Telecompaper*, *www.telecompaper.com/news/telia-to-re-assess-position-in-latvia-after-cooperation-with-govt-stalls--1309230*.

The Baltic Course (2018), *Baltics Keen to Test Self-Driving Cars on Via Baltica*, The Baltic Course, *www.baltic-course.com/eng/good_for_business/?doc=143975*.

Weller, D. and B. Woodcock (2013), "Internet traffic exchange: Market developments and policy challenges", *OECD Digital Economy Papers*, No. 207, OECD Publishing, Paris, *http://dx.doi.org/10.1787/5k918gpt130q-en*.

Notes

Israel
The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

1. Available at: *https://docs.google.com/spreadsheets/d/18ztPX_ysWYqEhJlf2SKQQsTNRbkwoxPSfaC6ScEZAG8/edit#gid=0*.
2. The Network Solutions Department (NIC) of the Institute of Mathematics and Computer Science, University of Latvia is the top-level domain .lv registry.

Chapter 4

FOSTERING THE DIGITAL TRANSFORMATION AMONG PEOPLE, FIRMS AND GOVERNMENT

On 21 August 1991, the Republic of Latvia declared the restoration of independence, only two weeks after the world's first website went online. Latvia has overcome many challenges since, such as the 2008 international financial crisis, and new challenges lie in the future such as a shrinking working age population, and addressing the fallout of the COVID-19. Raising productivity and fostering use of digital technologies can help in meeting these challenges.

Latvia has advanced strongly in Internet usage. The government is a leading user among European countries of digital technologies, but the private sector lags far behind. Developing a comprehensive national digital strategy, with an adequate level of resources, can help Latvia further increase the usage of digital technologies by individuals, firms and government, as discussed in this chapter. The chapter examines individual usage, obstacles to more sophisticated use, and policies to increase usage (e.g. improving basic digital skills) including during the COVID-19 pandemic. It explores the low use of digital technologies among firms, especially e-commerce, current policies to increase digital skills in the workplace and programmes to encourage digital uptake among firms. Finally, the chapter looks at steps being taken to increase usage of digital technologies in government and provides policy recommendations.

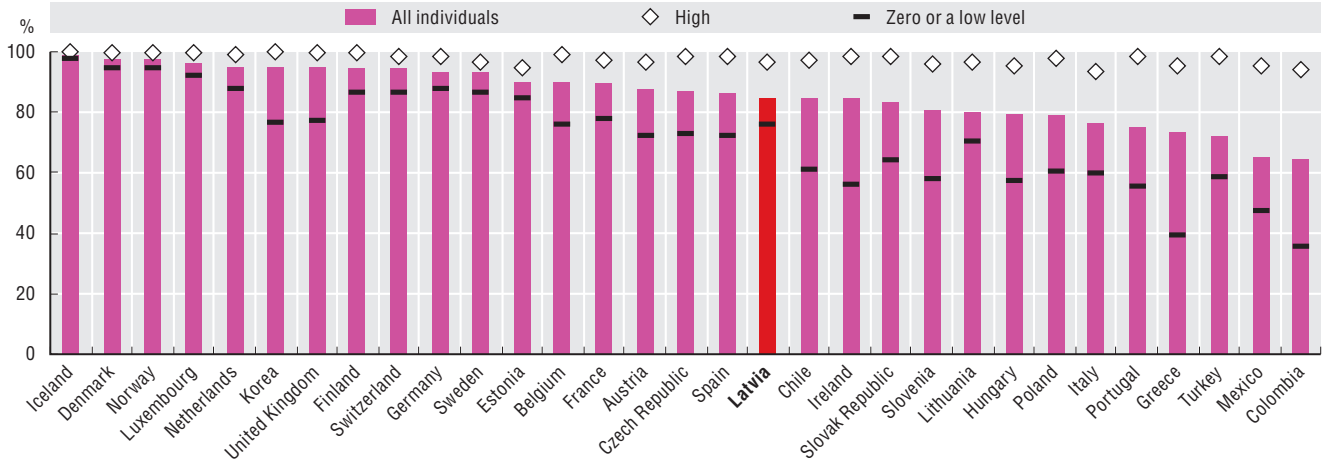
Usage of digital technologies by individuals

Internet use by group

Latvia's population are moderate Internet users, in line with the trend in neighbouring countries with a similar level of GDP (Figure 4.1). Differences exist among demographic groups (based on age, education and gender), but are also mirror those of peer countries (Figure 4.2). Narrowing such differences is essential to achieving the goals of the Information Society Development Guidelines (see Chapter 7).

Figure 4.1. Internet users by educational level in selected OECD countries, 2018 or latest available year

As a percentage of all individuals aged 16-74 in each category



Notes: Unless otherwise stated, Internet users are defined for a recall period of three months. For Colombia, the recall period is 12 months. For the United States, no time period is specified.

Source: OECD (2018a), *ICT Access and Usage by Households and Individuals* (database), *http://oe.cd/hhind* (accessed in March 2020).

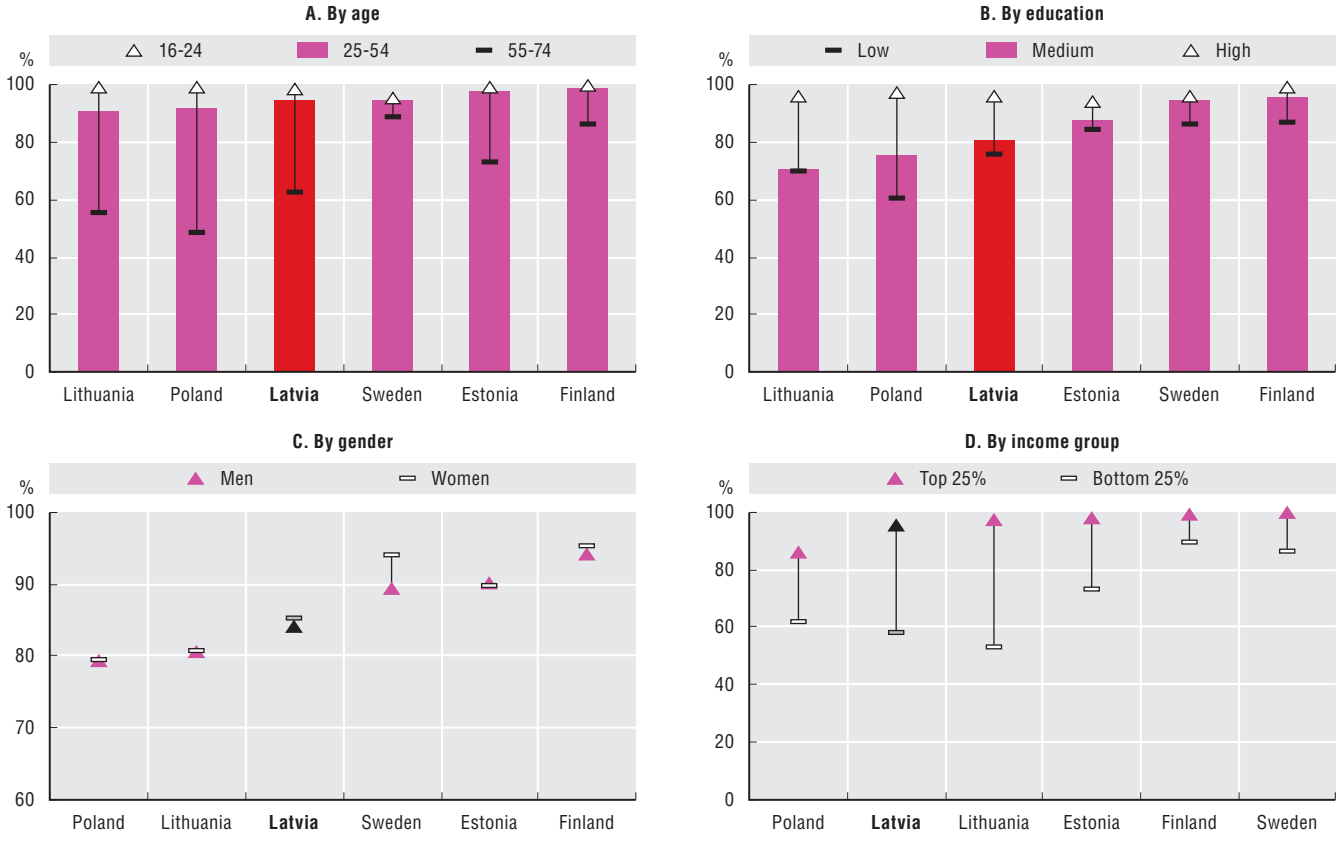
However, in recent years adoption of the Internet has proceeded at a gradual pace (Figure 4.3), with the share of individuals using the Internet weekly at a slower rate than the EU average (European Commission, 2018a). This trend can be explained in part by stagnation in adoption among those on lower incomes, as differences based on age and education have been narrowing (Figure 4.4).

In addition, a fifth of households lack a broadband connection (Figure 5.5). Many households indicate a low demand for Internet access at home: although the most common reason households claim for not having access to the Internet at home is a lack of need, cost and a lack of skills as factors, especially in

poorer households. The reported lack of need for Internet access among poorer households can reflect a lack of awareness of its benefits or different priorities (Figure 4.6). This low rate of connection applies to both rural and urban households (Figure 4.7).

Figure 4.2. Internet users by category in selected OECD countries, 2018 or latest available year

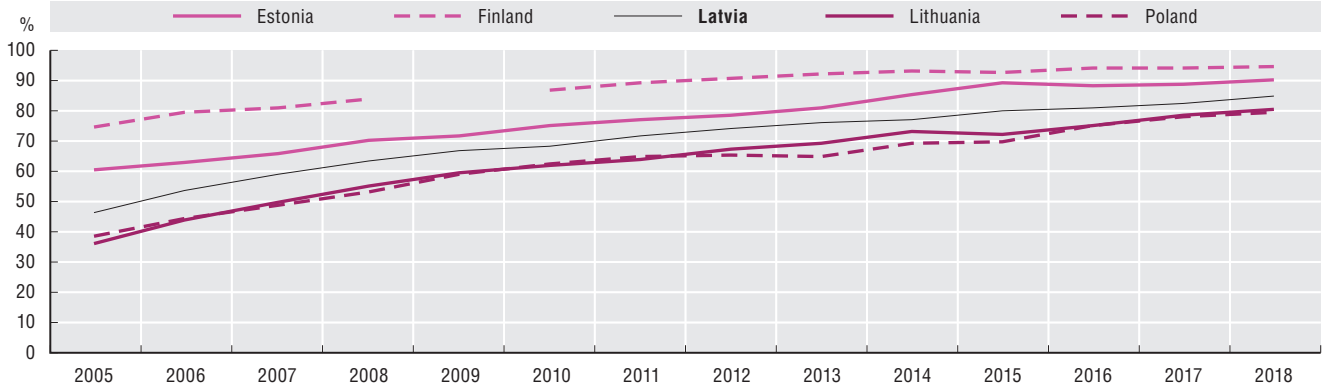
As a percentage of all individuals aged 16-74 in each category



Source: OECD (2018a), *ICT Access and Usage by Households and Individuals* (database), *http://oe.cd/hhind* (accessed in March 2020).

Figure 4.3. Trends in Internet users in Latvia and selected OECD countries, 2005-18

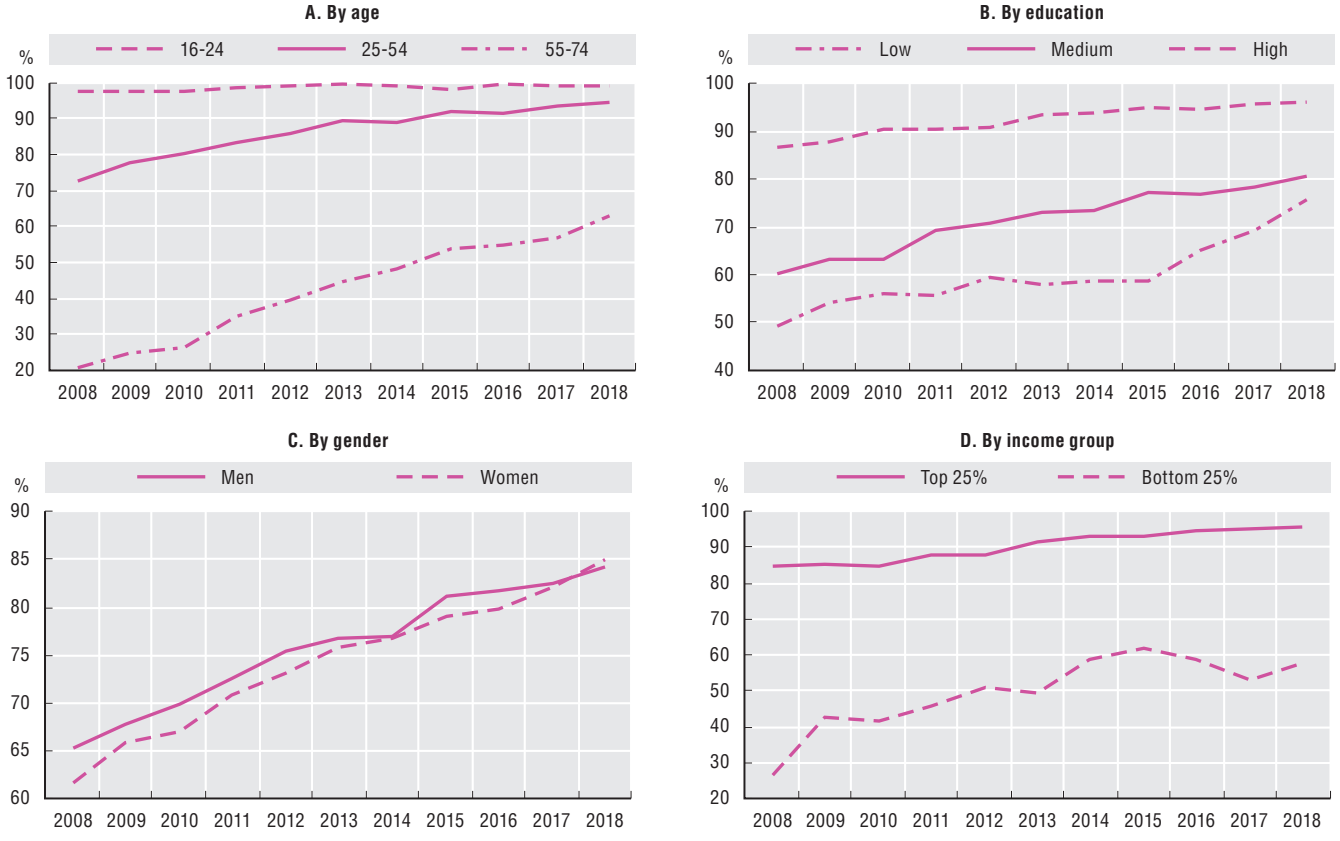
As a percentage of all individuals aged 16-74



Source: OECD (2018a), *ICT Access and Usage by Households and Individuals* (database), *http://oe.cd/hhind* (accessed in March 2020).

Figure 4.4. Trends in Internet users by category in Latvia, 2008-18

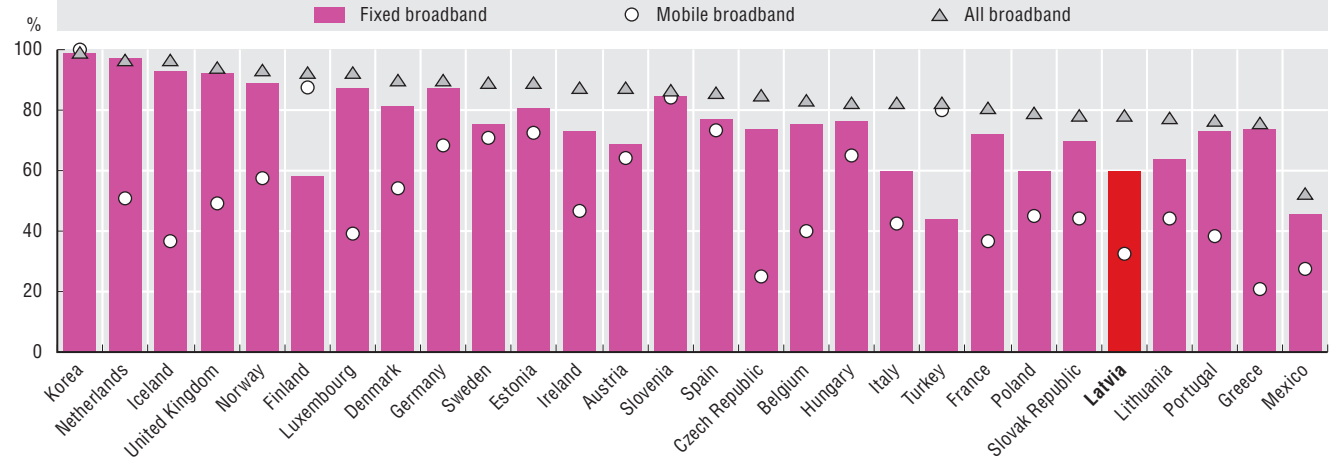
As a percentage of all individuals aged 16-74 in each category



Source: OECD (2018a), *ICT Access and Usage by Households and Individuals* (database), *http://oe.cd/hhind* (accessed in March 2020).

Figure 4.5. Internet access at home in selected OECD countries, 2018

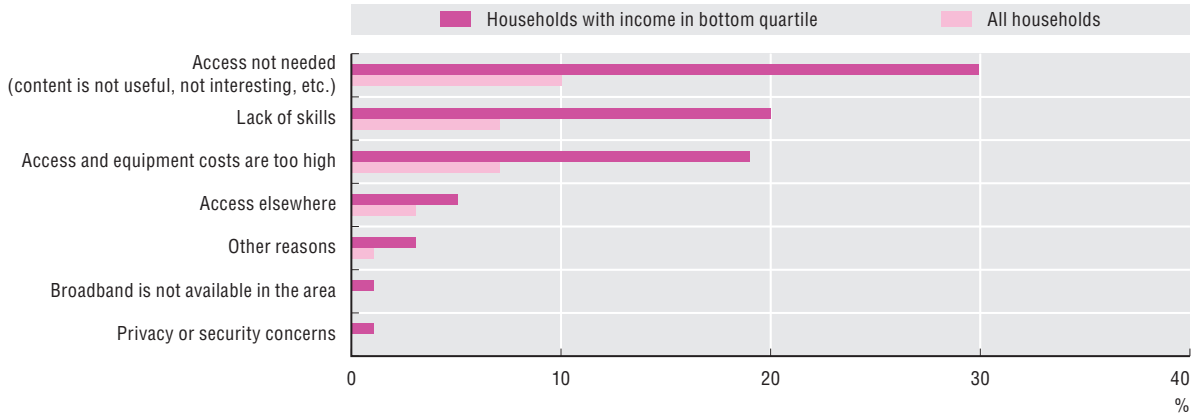
As a percentage of households with broadband access at home



Source: OECD (2018a), *ICT Access and Usage by Households and Individuals* (database), *http://oe.cd/hhind* (accessed in March 2020).

Figure 4.6. Reasons for not having Internet access at home in Latvia, 2018

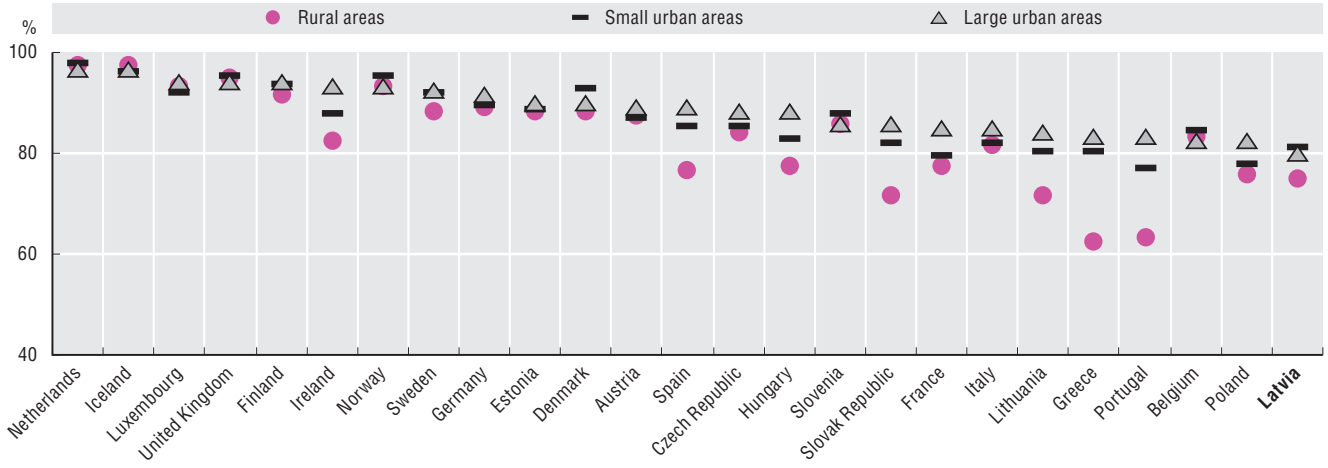
As a percentage of all households



Source: Eurostat (2020c), *ICT Usage in Households and by Individuals* (database), *https://ec.europa.eu/eurostat/cache/metadata/en/isoc_i_esms.htm*.

Figure 4.7. Rural-urban gap in broadband access in Latvia and selected OECD countries, 2018

Percentage of households with broadband access at home



Source: OECD (2018a), *ICT Access and Usage by Households and Individuals* (database), *http://oe.cd/hhind* (accessed in March 2020).

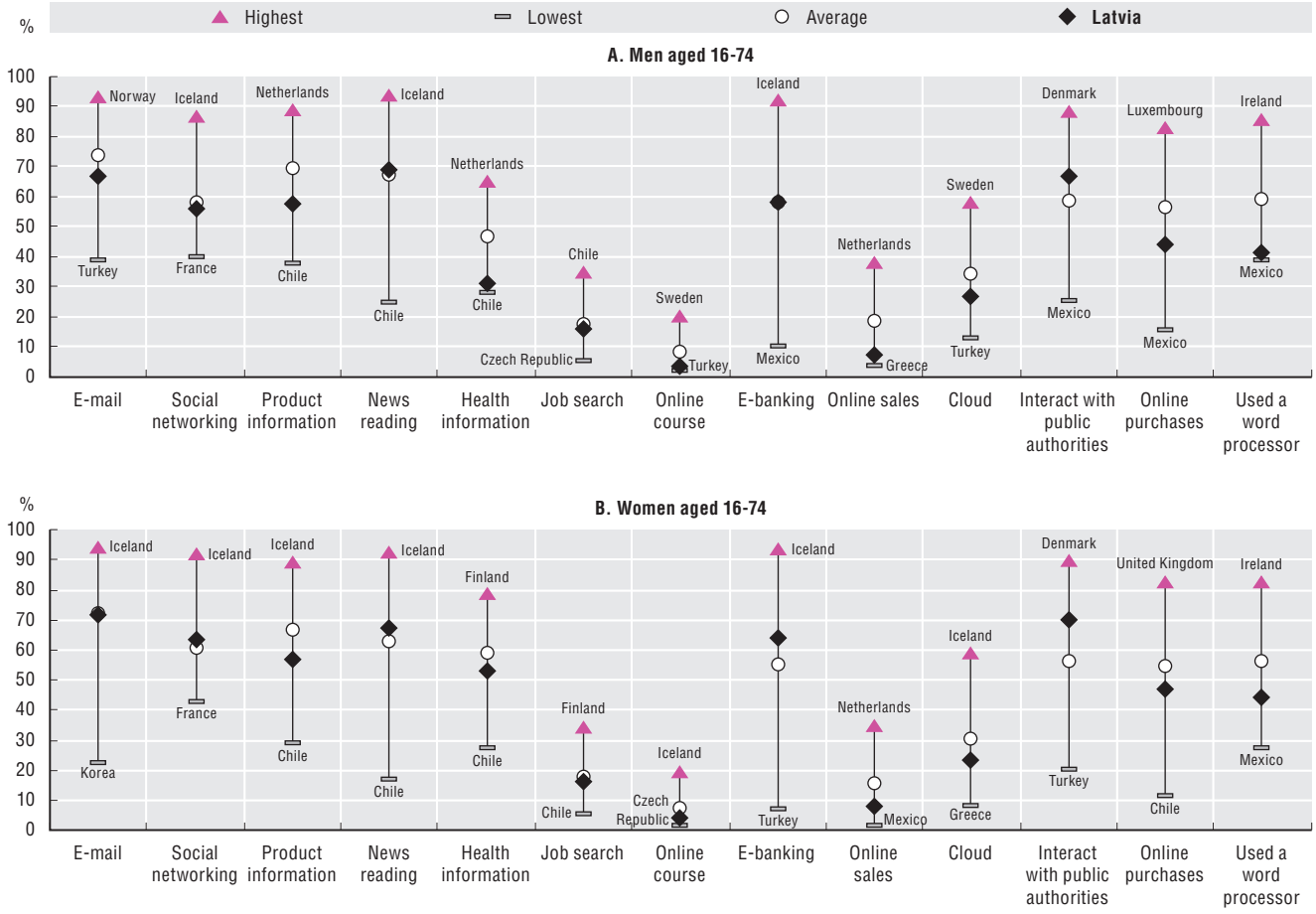
The uses individuals make of the Internet

Although a substantial proportion of Latvia's inhabitants do not use the Internet (see above), those who do make relatively diversified and complex use of the Internet (OECD, 2019a). Among Internet users, use of e-banking and interacting with public authorities is above the OECD average. However, few have taken online courses, in line with the overall low trend for participation in continuing education and training (see below). As with other OECD countries, minor gender differences persists in Internet usage, with women more likely to use social media than men, and considerably more likely to access health information (Figure 4.8).

However, Latvia lags behind other countries with a similar proportion of Internet users in terms of participation in e-commerce. Given the advanced level of participation in other activities (e.g. e-banking and interacting with public authorities), such low participation can be explained by the lack of Latvian firms selling online (see next subsection). Less than half of Internet users have made an online purchase in the past year and even fewer have made a sale online. This is in part due to the size of Latvia's older population, as purchases by those aged 16-24 is closer to the OECD average (OECD, 2018a). In addition, online purchases tend to be low in value (Figure 4.9). Latvia has already achieved the target of 35% of inhabitants buying online by 2020 (Information Society Development Guidelines, Chapter 6) (Eurostat, 2020a); therefore, a more ambitious target is appropriate.

Figure 4.8. Internet use by individuals in Latvia, 2017 or latest available year

As a percentage of Internet users performing each activity



Source: OECD (2018a), *ICT Access and Usage by Households and Individuals* (database), *http://oe.cd/hhind* (accessed in March 2020).

Promoting ICT usage among individuals

Several programmes are in place to encourage ICT usage among individuals. These focus mainly on providing individuals with the skills to use digital technologies effectively, but tend to be small in scale. The adoption of a community-based approach to promoting use of digital technologies, and combining this strategy with other strategies (e.g. connecting with the diaspora), could increase uptake.

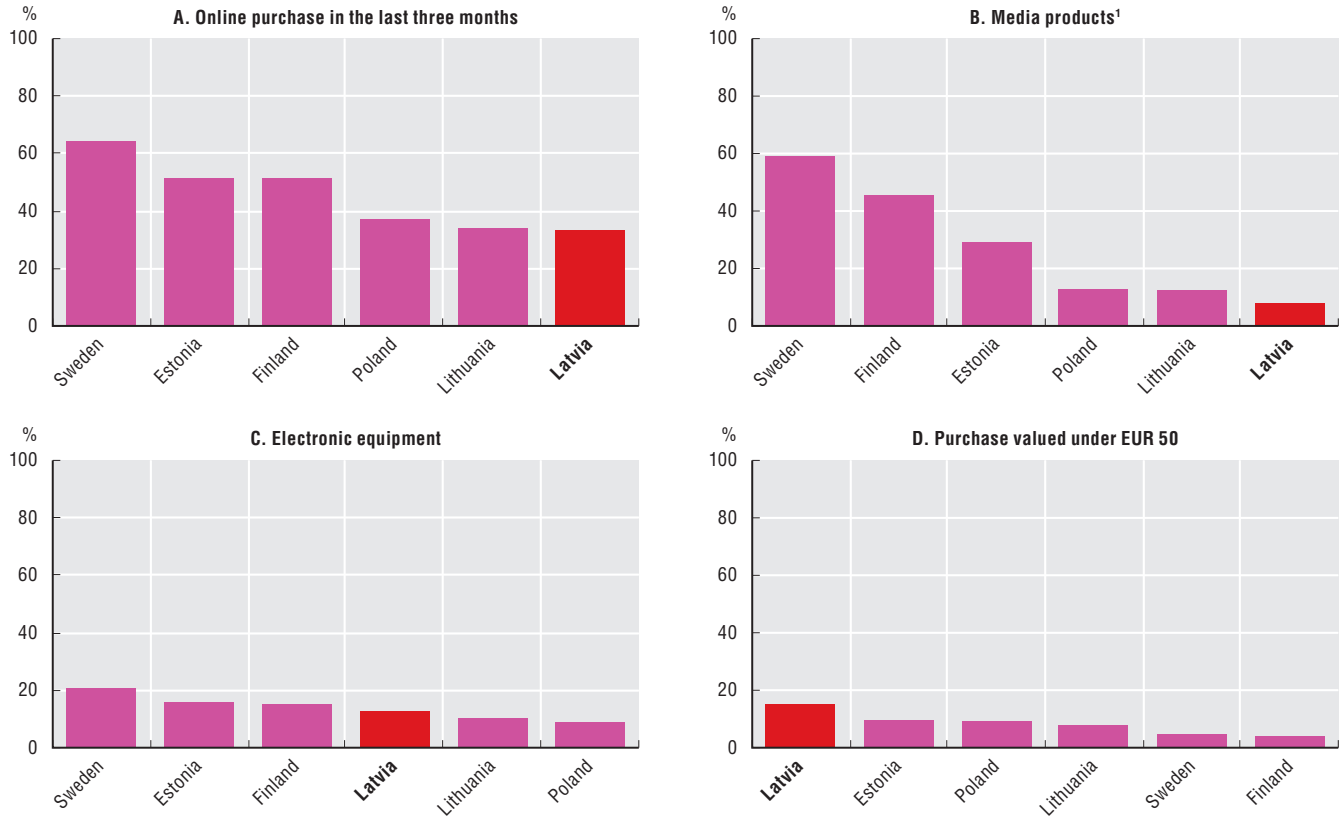
Since 2010, the Latvian government has aimed to raise awareness of the possibilities of ICTs through participation in European Digital week (previously E-skills week), which aims to inform the public of the benefits of improving their digital skills and the possibilities of training. In 2019, Digital Week was organised by the Latvian Information and Communication Technology Association (LIKTA) and the Ministry of Environmental Protection and Regional Development (Vides Aizsardzības un Reģionālās Attīstības Ministrija, VARAM), with over 500 events in 74 towns and cities (KISC, 2019a). In addition, Latvia has sought to increase the use of government e-services through the My Latvija.lv! Do Digitally! (Mana Latvija.lv Dari Digitali!) campaign (see below). Making use of web analytics to examine the effect of such programmes could help Latvia ensure that resources are used effectively.

The Ministry of Culture has sought to increase effective use of the Internet (in line with the Cultural Policy Guidelines "Creative Latvia 2014-2020") by promoting the creation of Latvian language online content. Latvia's Centre for Cultural Information Systems (Kultūras Informācijas Sistēmu Centrs, KISC) aims to preserve Latvia's cultural heritage by establishing digital archives of newspaper and journals as well as other materials such as historic posters, postcards and photographs, which are currently stored in Latvia's museums, archives and libraries (KISC, 2019b). In addition, the portal *biblioteka.lv*

allows people to access local content produced by public libraries, while a selection of Latvian language books and translations can be accessed for free via the 3td.lv online portal. KISC also provides training to librarians. In addition, the government has attempted to boost the amount of locally produced and Latvian language content, by developing translation tools, grammar correctors and online terminology databases.

Figure 4.9. Online purchases in Latvia and selected OECD countries, 2018

As a percentage of all individuals



1. Media products include films and music; or books, magazines and e-learning material; and computer software.

Source: Eurostat (2020c), *ICT Usage in Households and by Individuals* (database), *https://ec.europa.eu/eurostat/cache/metadata/en/isoc_i_esms.htm*.

As in many other countries, distant learning has been key to sustaining education in Latvia during the shutdown following the COVID-19 pandemic. Despite the challenges raised by the sudden shift from in-person teaching to e-learning, distant learning has accelerated digital uptake in education dramatically, with effects that are likely to persist after the crisis (see Box 4.1).

Box 4.1. Distant learning during the COVID-19 pandemic

On 12 March 2020, the Latvian government declared a state of emergency and closed all schools, immediately raising the challenge of how to continue educating children in Latvia. The education system responded by delivering distance learning utilising a mixture of traditional and digital tools.

The Ministry of Education and Science (MoES) prioritised the continuity of academic learning and support for teachers and students who lack the skills for online or independent study. Accordingly, the National Centre for Education developed guidelines for the implementation of distance learning, providing advice and guidebooks for parents and teachers online.

Box 4.1. Distant learning during the COVID-19 pandemic *(cont.)*

Guidelines for evaluating students were also issued and included recommendations to allow students greater flexibility in demonstrating their abilities (e.g. writing or creating videos). In addition, schools have been given the autonomy to prioritise the aspects of the curriculum they deem most appropriate (MoES, 2020).

A mix of technologies have been used to deliver the curriculum. Approximately 440 hours of lessons for primary and secondary students have been broadcast on free-to-air television, with sign language available for children with hearing difficulties. In addition, students can access lessons via the Your class (Tava klase) website, while teachers have made use of tools such as Edurio to give tests and questionnaires, as well as widely used applications such as WhatsApp. Finally, the National Film Centre of Latvia has allowed free access to films related to the curriculum for Latvian students.

Given the existence of a digital divide, there was a risk that some children could be left behind. To address this possibility, the MoES has made digital devices available to the approximately 5 000 students (about 3% of all school pupils) who lacked access to such tools. In addition, some schools have prepared and distributed packages of printed materials to pupils.

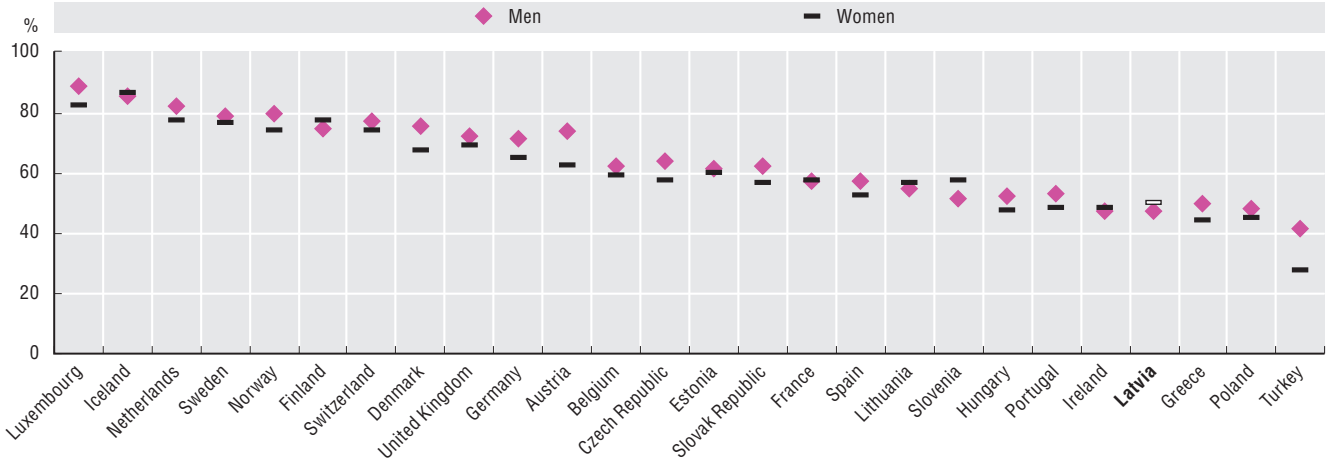
While digital technologies are not a substitute for traditional classrooms, they do provide certain benefits, including making activities such as homework more interactive and effective as a learning tool. Latvia has been monitoring distance learning through the use of weekly surveys, and the lessons learned from the use of digital technologies may influence how education is delivered in the future.

Improving skills forms an important part of efforts to increase ICT usage

Absence of basic digital skills hinders greater use of ICTs by individuals, with half of the adult population in Latvia lacking such skills (e.g. the ability to move or copy files between folders) (Figure 4.10). Gender differences in this area are minor, although a greater share of women (30%) have above basic skills than men (24%), in contrast to other EU countries (Eurostat, 2019a). In addition, differences between rural and urban areas are moderate (Figure 4.11).

Figure 4.10. Individuals with basic or above basic digital skills[1] in Latvia and selected OECD countries, by sex, 2017

As a percentage of all individuals



1. Those with basic skills have performed one of the following tasks: copied or moved files or folders, saved files on Internet storage space, obtained information from public authorities/services' websites, found information about goods or services, and sought health-related information. "Above basic digital skills" refers to the ability to perform two or more such activities.

Source: Eurostat (2020c), *ICT Usage in Households and by Individuals* (database), *https://ec.europa.eu/eurostat/cache/metadata/en/isoc_i_esms.htm*.

Figure 4.11. Rural–urban gap in digital skills in Latvia and selected OECD countries, 2017

Individuals with basic or above basic digital skills,[1] as a percentage of all individuals

1. Those with basic skills have performed one of the following tasks: copied or moved files or folders, saved files on Internet storage space, obtained information from public authorities/services' websites, found information about goods or services, and sought health-related information. "Above basic skills" refers to the ability to perform two or more such activities.

Source: Eurostat (2020c), *ICT Usage in Households and by Individuals* (database), *https://ec.europa.eu/eurostat/cache/metadata/en/isoc_i_esms.htm*.

Improving ICT education and e-skills is a core focus of the Information Society Development Guidelines. Programmes have been created to improve the basic skills of users, in addition to providing training in more advanced skills sought by employers (see section below). The government has developed several policies to promote digital literacy among adults in Latvia, which have been implemented through the network of public libraries.

Public libraries act as free access points for the Internet and as centres for the development of basic digital skills. In 2008, KISC received funding from the Bill & Melinda Gates Foundation and the Latvian government to provide 4 000 computers to Latvia's public libraries as part of the Third Father's Son (Trešais Tēva Dēls) programme. Broadband connections were provided for libraries, and free Wi-Fi was made available. Librarians were trained to assist users and a training programme on basic IT skills was developed targeting those with low levels of income and education, rural inhabitants and older citizens, with a similar programme developed for children (KISC, 2015). In addition, over 450 public Wi-Fi hotspots were created (managed by 76 municipalities) as part of an ERDF-funded project (over 4 400 free Wi-Fi spots are also available which do not receive public funding).

The Third Father's Son programme has proven successful, however the responsibility for replacing equipment and providing basic ICT training has fallen to municipalities. In addition, many of the online training materials (available on the KISC website) are now outdated. Updating these materials would help to ensure that libraries can continue to offer help to those who wish to acquire basic digital skills. In addition, municipalities should be obliged to ensure that equipment is maintained and replaced as required, with funding made available from central sources.

However, given the low level of digital skills among the Latvian population, greater efforts are warranted. At present, most resources for developing basic digital skills are targeted at school-going children (see below). In Colombia, an initiative to link programmes to develop digital skills among children with evening programmes to develop the skills of their parents proved successful, and could also be beneficial in Latvia (OECD, 2019b).

Latvia should build on the success of the Third Father's Son programme by creating a community-based programme to boost the digital skills of those in more rural locations and older Latvians. Although a programme of "digital agents" exists, this focuses on promoting the use of government digital services rather than more general usage. Instead, Latvia should give grants to partners, such as NGOs or local community groups, in order to train digital mentors to highlight the benefits of ICTs, an approach that has proven successful in Australia and Norway (Box 4.2). Latvia should first

work with focus groups consisting of those make relatively little use of ICTs (e.g. the elderly), to discover the barriers they face and to examine the ways in which greater use of digital technologies would benefit them. The outcomes would feed into the development of a training programme to be delivered by digital mentors.

Box 4.2. Australia and Norway take community-based approaches to encouraging digital literacy among adults

The Australian Be Connected programme aims to raise the digital literacy of older Australians, and to address social problems by reducing feelings of loneliness and increasing community connection. The Department of Social Services gives grants to 2 500 local partners (e.g. community organisations) to train digital mentors who then take a community-centred approach to teaching basic skills such as online shopping, sending e-mail and using social media.

In Norway, the Digidel programme of 2017 aimed to promote digital literacy and inclusion. Focus groups centred around groups that do not regularly use ICTs (including the elderly and immigrants), were created to understand the barriers they face and how they might benefit from using these tools. Training activities then took place facilitated by local libraries, NGOs and firms.

Given the stated government goal of strengthening connections with the Latvian diaspora, Latvia could exploit digital technologies to interact with members of the diaspora digitally (Cross-sectoral Coordination Centre, 2017). The first stage of this initiative would involve training Latvia's older inhabitants to use social media, to enable them to maintain contact with relatives abroad. Basic use of the Internet can serve as a gateway for more sophisticated use by Latvia's inhabitants. The second stage of the initiative would require active promotion through social media of online content maintained by KISC.

Usage by individuals: Conclusions

Latvia's continued efforts to increase the share of individuals making effective use of the Internet have resulted in progress, although a sizeable minority still lack basic skills. Libraries and community-based programmes can help provide these people with the digital skills they lack. In addition, greater use of existing resources can be made to establish virtual links with the Latvian diaspora abroad. The recommendations in this section are summarised in Box 4.10.

However, in order to increase the participation of consumers in e-commerce, it will be necessary to increase the share of Latvian firms that make effective use of digital technologies. This issue is discussed in the following section.

Usage of digital technologies by firms

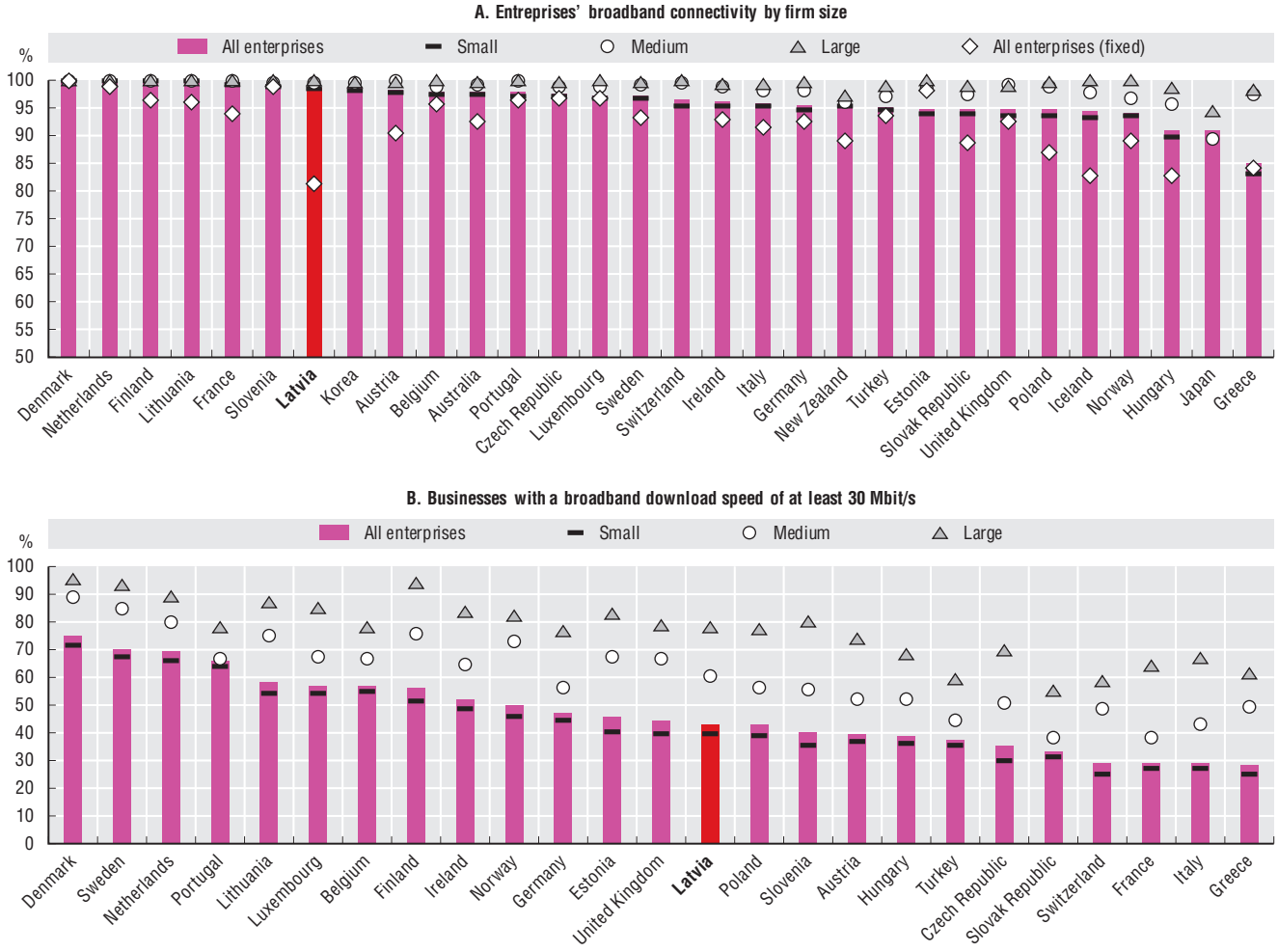
In order to raise living standards, it is necessary for Latvia to raise economic growth and productivity. Latvian industry has a large proportion of low-tech firms and labour productivity lags behind neighbouring Baltic countries, due to a slowdown in productivity growth following the financial crisis (European Commission, 2018b; OECD, 2019c). In addition, the wide dispersion of productivity among firms, especially in the administration and support sectors, suggests that only a few advanced firms are making use of new technologies (OECD, 2019c). Greater adoption of digital technologies, especially among smaller firms, has the potential to help raise productivity.

Current rate of ICT usage by firms

Latvian firms lag behind those of other OECD countries in their use of ICTs. Although most firms are connected by broadband to the Internet, a relatively low share (80%) have fixed connections (which tend to offer higher speeds), leading overall to moderate connection speeds (Figure 4.12).

Figure 4.12. Business connections to fixed broadband in Latvia and selected OECD countries, 2018 or latest available year

As a percentage of all firms with ten or more employed persons



Notes: Only enterprises with ten or more employees are considered. Size classes are defined as: small (10-49 employees), medium (50-249 employees) and large (250 employees or more). For Japan, data refer to businesses with 100 or more employees instead of 10 or more; medium-sized enterprises have 100 to 299 employees and large ones 300 or more.

Source: OECD (2018a), *ICT Access and Usage by Businesses* (database), *http://oe.cd/bus* (accessed in March 2019).

In addition, involvement among firms in e-commerce remains low, despite the willingness of Latvians to engage in a broad range of Internet uses, such as e-banking (Figure 4.13). Latvia lags behind the OECD average in terms of the number of firms with a website, and although the number of firms that make e-purchases is in line with the OECD average, the share of firm turnover generated from web sales is among the lowest in the European Union (Figure 4.14). Indeed, Latvian firms are unlikely to achieve the target of 15% of turnover coming from Internet sales by 2020, as set out in the Information Society Development Guidelines.

In addition, Latvia lags further behind the OECD average in terms of the use of more sophisticated technologies such as enterprise resource planning (ERP) software, the use of customer relationship management (CRM) software and radio-frequency identification (RFID) technology (Figure 4.15) (OECD, 2018b).

Figure 4.13. Internet use by businesses in selected OECD countries, 2018 or latest available year

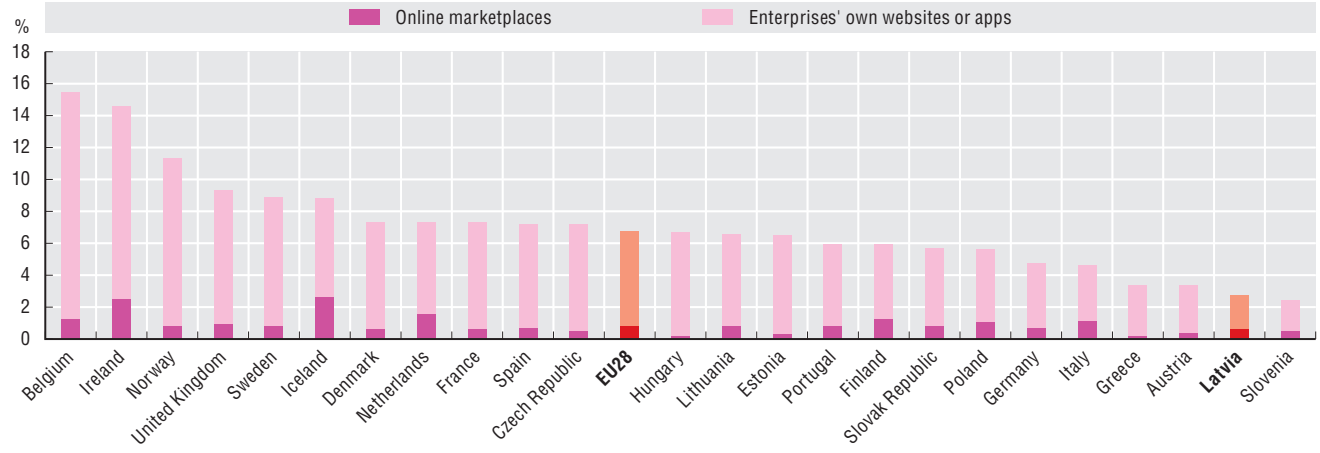
As a percentage of all firms with ten or more employed persons

Note: Only enterprises with ten or more employees are considered.

Source: OECD (2018a), *ICT Access and Usage by Businesses* (database), *http://oe.cd/bus* (accessed in March 2019).

Figure 4.14. Turnover from web sales in Latvia and selected OECD countries, 2017

As a percentage of total turnover



Source: Eurostat (2019c), *E-Commerce Statistics* (database), *https://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics*.

Obstacles to greater usage of digital technologies

Adoption of ICTs is held back by a variety of factors. These include a large proportion of small firms, which tend have lower ICT adoption rates; an absence of workers with adequate skills to take full advantage of ICTs; and a lack of workers with complementary skills such as management needed to transform work practices in firms.

Latvia has a large proportion of small firms

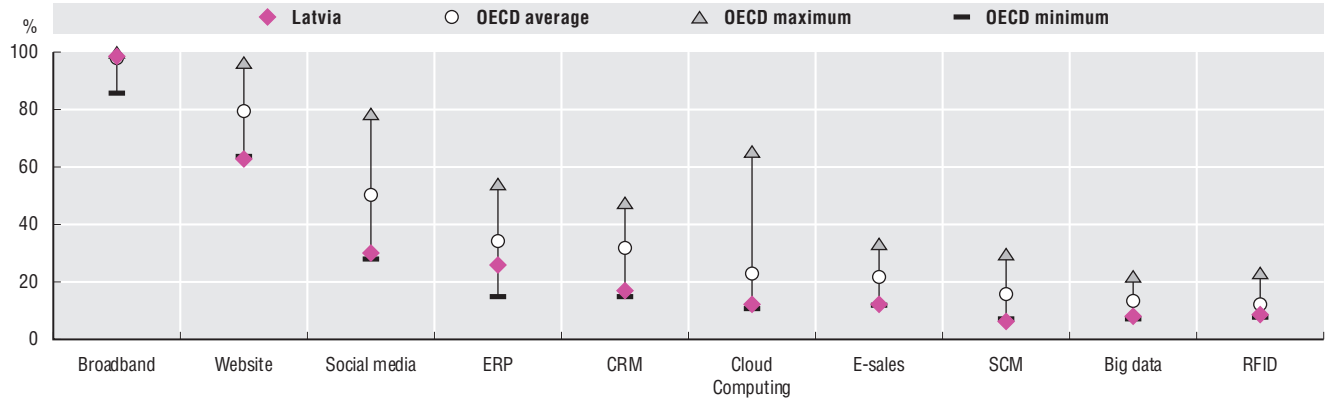
Latvia has a large share of micro and small firms, with employment concentrated in the latter (Figure 4.16).

Smaller firms face barriers to the adoption of ICTs, including difficulties accessing finance with which to invest in ICTs. Lending to SMEs has remained low since the financial crisis (OECD, 2019d). In addition, relatively few firms are managed by professional managers (instead being run by family members), which can hinder the adoption of modern managerial approaches that are complementary to digital technologies (Figure 4.18) (Andrews, Nicoletti and Timiliotis, 2018; OECD, 2019c). Indeed, Latvia has a shortage of professionals with managerial and administrative skills (Figure 4.19). As a result, a large

pool of small firms have shown no productivity growth in recent years, suggesting a lack of ability to absorb new technologies (OECD, 2019c). Indeed, Latvia's SMEs have been reluctant to make even basic use of digital technologies, such as the use of social media (Figure 4.17).

Figure 4.15. Business use of advanced digital technologies in selected OECD countries, 2017 or latest available year

As a percentage of all firms with ten or more employed persons

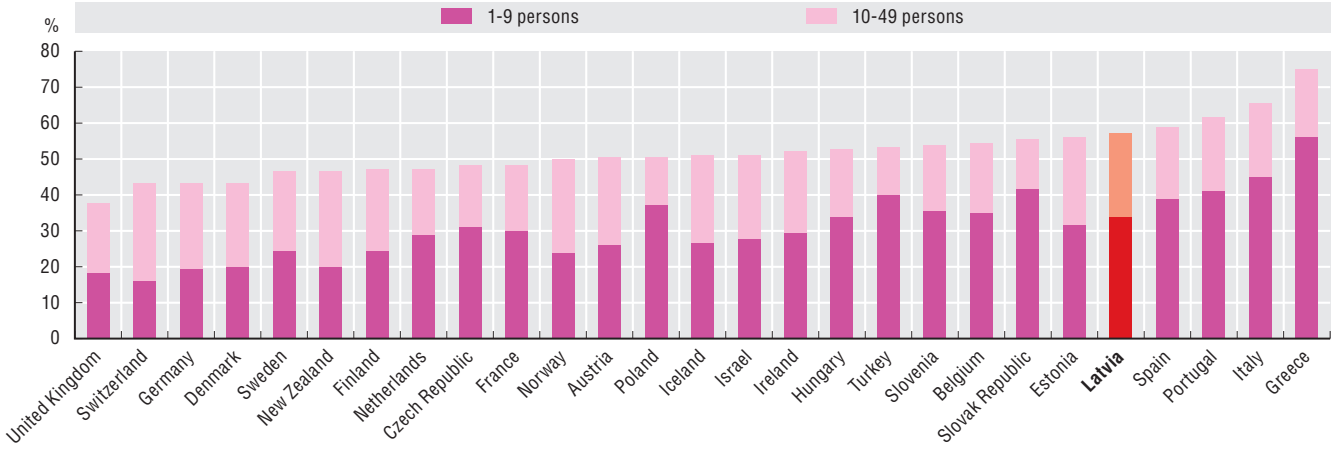


Notes: Data cover 26 OECD countries and correspond to the share of businesses with ten or more employees a with broadband connection (fixed or mobile), with a website or home page, using social media, using enterprise resource planning (ERP) software, using customer relationship management (CRM) software, purchasing cloud computing services, receiving orders over computer networks, sharing electronically information with suppliers and customers (SCM), using radio-frequency identification (RFID) technology and having performed big data analysis (2018 data).

Source: OECD (2017c), *ICT Access and Usage by Businesses* (database), *http://oe.cd/bus*; Eurostat (2020c), *ICT Usage in Households and by Individuals* (database), *https://ec.europa.eu/eurostat/cache/metadata/en/isoc_i_esms.htm*.

Figure 4.16. Employment by firm size in Latvia and selected OECD countries, 2016

As a percentage of all persons employed

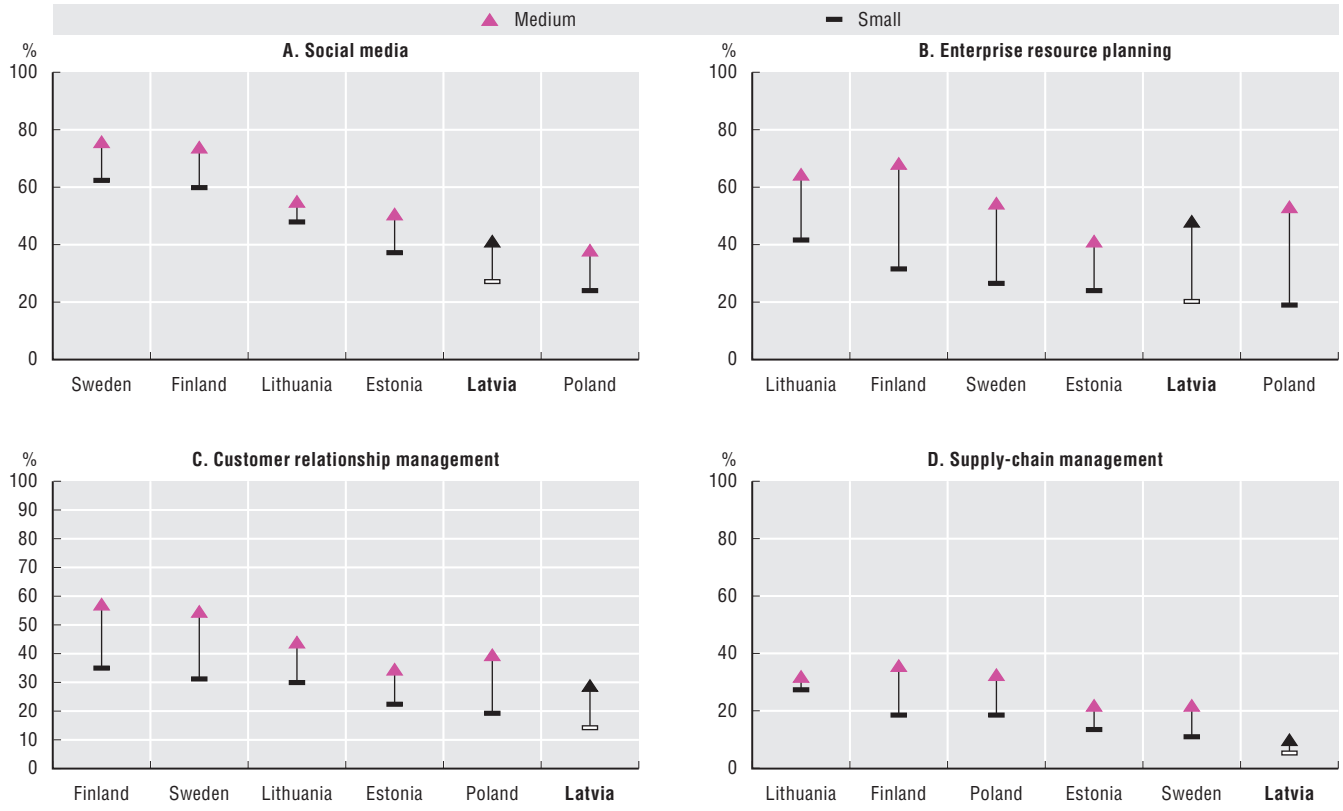


Source: OECD (2020), *OECD Structural and Demographic Business Statistics (SDBS)* (database), *https://stats.oecd.org/Index.aspx?DataSetCode=SSIS_BSC_ISIC4* (accessed on 6 May 2020).

The large share of small firms can, in part, be explained by a reduced 15% microenterprise tax regime, which includes social security and personal tax, including for employees (OECD, 2019e). To qualify, the firm must not employ more than five people, the monthly income of any employee cannot exceed EUR 720 (compared to a minimum wage of EUR 430), and firm turnover must not exceed EUR 40 000 (reduced from EUR 100 000 in 2018) (MoF, 2018). This discourages firms from growing above these thresholds, and can lead to firms under-declaring their income (Jacobs et al., 2017).

Figure 4.17. Use of advanced digital technologies by firm size in Latvia and selected OECD countries, 2017

As a percentage of all firms with ten or more employed persons

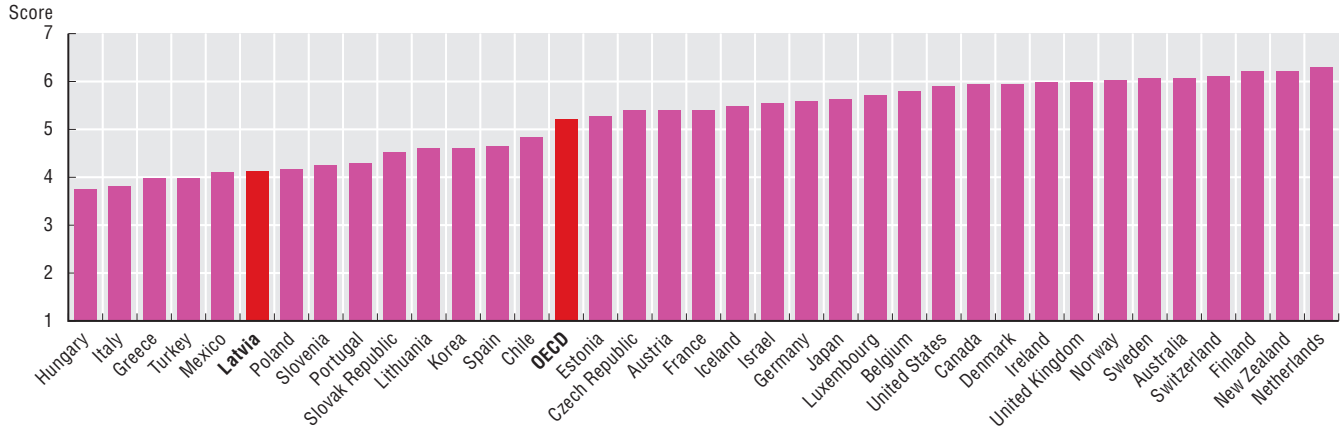


Note: Size classes are defined as: small (10-49 employees) and medium (50-249 employees).

Source: OECD (2017c), *ICT Access and Usage by Businesses* (database), *http://oe.cd/bus* (accessed in February 2020).

Latvia also has a high degree of informality, which can hinder the adoption of digital technologies. The informal economy in Latvia is estimated to represent almost 25% of GDP, with 10% of employees not reported to the authorities, many of whom are migrant workers (Sauka and Putniņš, 2019). Informality can inhibit digitalisation as informal firms may wish to remain small to avoid detection, while the under-declaration of income can lead to unwillingness among banks to lend money (Perry, 2017; OECD, 2019c).

Figure 4.18. Reliance on professional management in selected OECD countries, 2017-18



Note: Score based on responses to the question: "In your country, who holds senior management positions in companies? [1 = usually relatives or friends without regard to merit; 7 = mostly professional managers chosen for merit and qualifications]".

Source: World Economic Forum (2017), *The Global Competitiveness Index Historical Dataset 2007-2017*, *https://tcdata360.worldbank.org/indicators/fin.loc.eqy.mkt?country=BRA&indicator=525&viz=line_chart&years=2007,2017*.

Digital technologies are being used in Latvia to reduce informality. For example, it is now compulsory for construction firms to electronically record the working hours of workers and to register all those who enter a construction site (e.g. through the use of a card or mobile device). The resulting data are uploaded to a central database (VEDLUDB) which can be access by the tax authorities (OECD, 2019c). In addition, in 2017 a plan was launched that made electronic record-keeping cash registers compulsory, with 88% of such devices replaced by September 2019. The State Revenue Service has also been using ICTs to better target people for tax audits (OECD, 2019c). Latvia could build on this progress by creating a system of automatically reporting payroll information, similar to Australia's Single Touch Payroll system. Under this system, business payroll software automatically reports data to Australia's tax authorities as employees are paid, reducing compliance costs for businesses and individuals, and enabling earlier detection of firms that do not meet their tax and social security obligations (Australian Taxation Office, 2019).

Laws have also been changed to remove obstacles to the use of digital technologies and to reduce the cost of complying with regulations. Red tape has been reduced for businesses, for example through the use of online one-stop-shops for setting up firms (OECD, 2017a). In 2015, the Electronic Document Law was amended to remove previous restrictions on the use of electronic signatures (e.g. for private businesses or family law), and online registrations of firms and electronic registration of property without a notary are now possible (OECD, 2017a). In addition, from 2019 digitally signed documents must be accepted by affiliates to the Latvian Council of Sworn Notaries (e.g. financial institutions), which will further reduce the need for notarised documents (Valdani Vicari and Associati, 2019).

Greater efforts are needed to promote the use of digital technologies in small firms

At present, Latvia is focused on increasing digital skills (see below) but lacks policies to increase the usage of digital technologies among small firms, as well as a strategy for digitalising the private sector. While several programmes exist, such as the X industry hackathon run by the Latvia IT Cluster, these are small in scale and tend to be incorporated into innovation policies (see Chapter 5). In part, this is a consequence of projects being chosen based on the availability of EU funding, rather than clear national priorities.

In order to promote the digital transformation, Latvia should develop a strategy for digitalising SMEs that focuses on creating conditions whereby SMEs are willing to adopt digital technologies and invest in complementary knowledge-based assets and digital security. These conditions include enablers (e.g. infrastructure and the regulatory environment), firm-drivers (e.g. the availability of finance and skills); and the existence of technologies (e.g. digital platforms and services that facilitate the use of AI and big data) (OECD, 2019f).

Expanding workshops that teach small businesses simple ways to engage in e-commerce (e.g. through the use of online platforms) could help boost the adoption of such technologies and help more efficient firms gain market share. In addition, Latvia could develop a nationally funded programme to promote the adoption of existing technologies among Latvian SMEs, and offer a number of grants to firms across different sectors. Such an approach would act as an impetus for competitors to adopt more efficient technologies and business practices. In addition, tax incentives could be offered to encourage small firms to invest in ICTs.

Given the hesitancy that Latvian SMEs have shown in adopting digital technologies, Latvia should select a small number of firms to act as "digital champions". This approach has already been used in Australia, where 15 small firms were chosen and given intensive support (Box 4.3). Successful Latvian SMEs from sectors with low digital uptake could be selected as "digital champions" and granted public support based on their proposal for digitalisation. The success of such "digital champions" would demonstrate the value of digital technologies and spur other firms to adopt them in order to maintain or increase their market share.

For sectors where several firms already use digital technologies, more support should be given to help laggard firms catch up with leading firms. Austria has already implemented this approach offering consultancy advice to firms on how to modernise (Box 4.3). In sectors where firms already face competition from highly digitalised firms, laggard firms should pay for this service.

Box 4.3. A wide range of supports are available to help firms digitalise

Countries offer a wide range of supports to help firms digitalise, ranging from grants that subsidise investments in digital technologies to training to help firms implement investments at their own cost.

Australia's Small Business Digital Champions project supports 100 small businesses. The project has a total budget of AUD 8.9 million, and provides up to AUD 18 500 in assistance, with additional support from partner firms. Of these small businesses, 15 were chosen as Digital Champions and received mentoring from high-profile business people to guide them through the digital transformation. This process is then documented and showcased online. The programme is complemented by the "Digital Solutions" programme of the Small Business Advisory Service, which focuses on firms in regional locations. SMEs pay a (subsidised) fee for advice on implementing digital technologies, such as websites, e-commerce, social media and small business software. The programme also offers advice on online security and data privacy.

In Denmark, the Danish Business Authority distributes grants (valued at approximately EUR 1 300) to 2 000 SMEs under the SMV:Digital programme. The grants are used for private consultancy to help the SMEs identify digital opportunities with a special focus on e-commerce, prepare business cases for digital transformation and implement digital solutions.

Portugal also has a grant scheme to assist SMEs with the use of digital technologies in fields such as e-commerce, online marketing, website development and big data. The grant covers 75% of eligible expenses up to EUR 7 500 for projects that take up to one year to implement (European Investment Bank, 2019).

Austria does not offer grants, but does help SMEs digitalise through the KMU Digital programme. The programme includes: 1) an online tool to allow firms assess their level of digital maturity; 2) an individual consultation to examine what can be improved and how; 3) a consultation focused on the specific needs of the firm (in areas such as e-commerce, IT security, data protection and digitalisation of internal processes); and 4) digital skills training courses for entrepreneurs and employees.

Finally, Chile's innovation agency recently launched the Digitalise Your SME (*Digitaliza tu Pyme*) programme to which provides e-commerce courses (78 hours of classroom experience), in which small business owners can learn about digital marketing, the use of social networks and electronic commerce. By the end of the programme, participants should understand processes associated with e-commerce such as the use of online platforms.

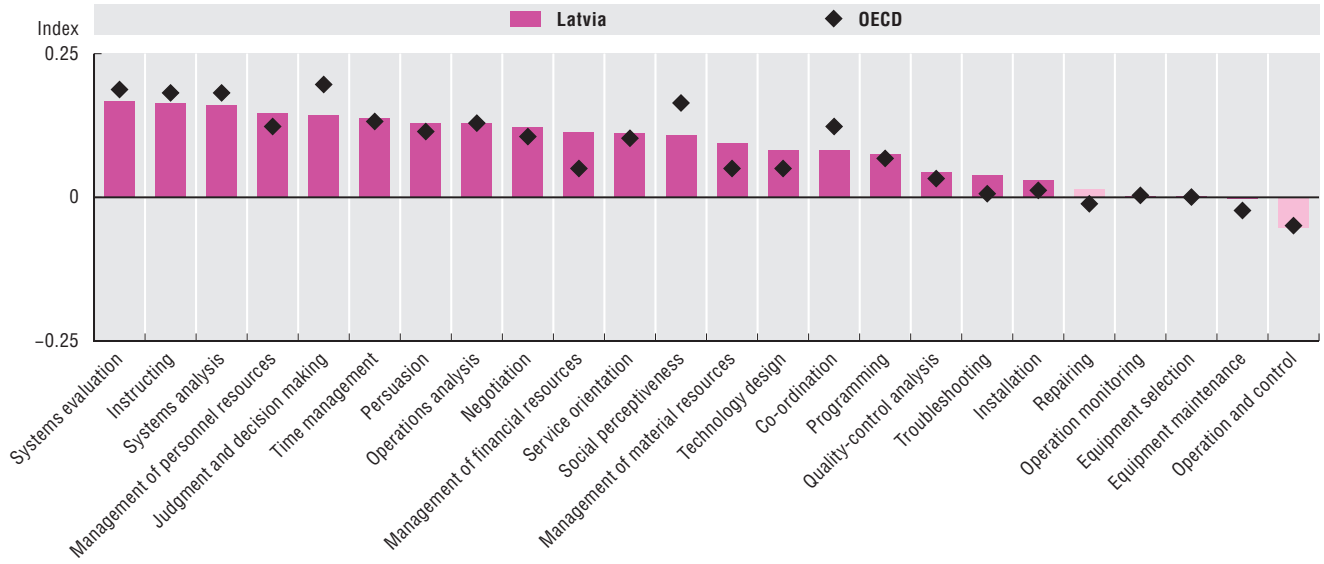
Source: Digital Economy Outlook policy questionnaire.

Skills required for the digital transformation

In order to increase the adoption of ICTs, Latvian firms need workers that have the necessary skills to make effective use of digital technologies. Improving skills has therefore been a main plank of the Latvian government's approach to increase the use of digital technologies among firms (Cross-sectoral Coordination Centre, 2017). Firms need workers with basic computer skills as well as ICT specialists to operate new systems. In addition, they require employees with advanced literacy and numeracy skills and workers with a tertiary education, in order to profit from the new working methods introduced by digitalisation. However, there is no single strategy for skills development; instead, there are varying strategies targeting different education levels and devised for different purposes (e.g. training teachers and promoting cybersecurity) (European Commission, 2019a).

Latvia will need to increase the number of workers with basic computer skills and the number of ICT specialists in order to sustain the digital transformation. The ability to use ICTs was a prerequisite or preferred in over half of job vacancies in 2018, although over half of those in Latvia lack even basic digital skills (EURES, 2018) (Figure 4.10). In addition, there is a shortage of workers with a knowledge of computers and electronics (Figure 4.19). Finally, ICT graduates earn a high wage premium, indicating substantial demand for their skills (Figure 4.20).

Figure 4.19. Skill shortages in Latvia, 2017

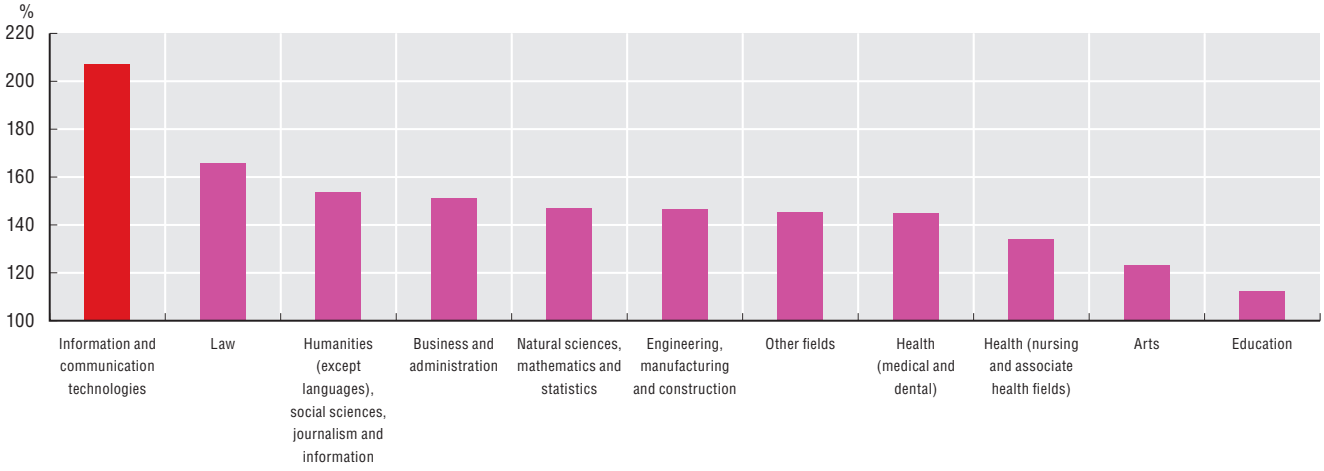


Note: Skills shortages (positive values) occur when the skills sought by employers are not available in the pool of potential recruits, whereas skills surpluses (negative values) occur when the supply of certain skills is higher than the demand for them.

Source: OECD (2018c), *Skills for Jobs – Latvia Country Note*, *www.oecdskillsforjobsdatabase.org/data/country_notes/Latvia%20country%20note.pdf*.

Figure 4.20. Relative earnings of tertiary-educated adults in the OECD, by field of study, 2017

25-64 year-olds with income from employment (full and part-time workers); upper secondary education (all fields) = 100

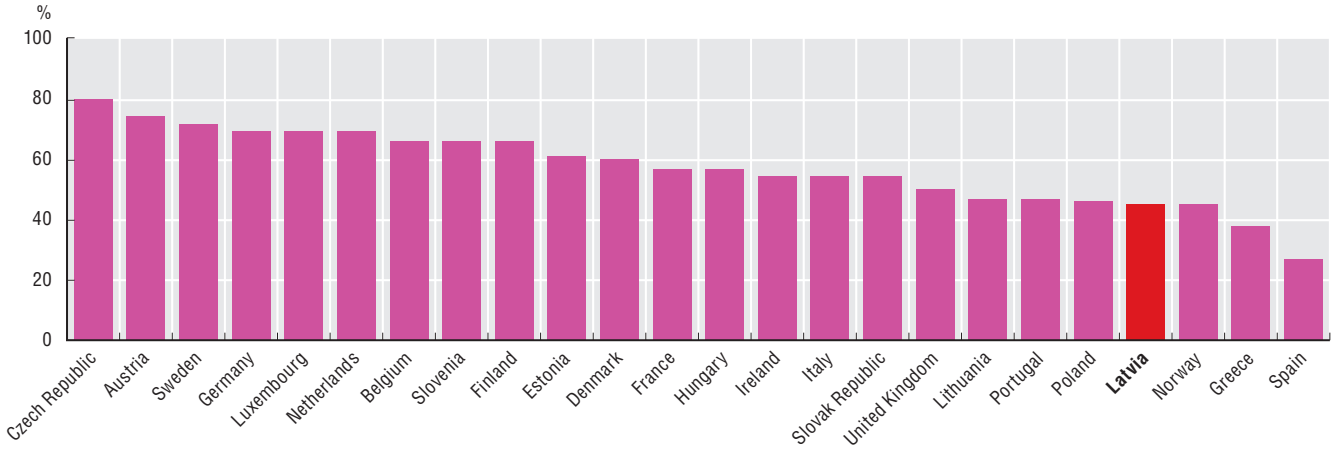


Source: OECD (2019g), *Education at a Glance: OECD Indicators*, *https://dx.doi.org/10.1787/f8d7880d-en*.

Nevertheless, it seems unlikely that the Latvian economy is ready to absorb the 3 000 new ICT graduates per year set as a target by the MoE (2018). The proportion of working age graduates with an ICT qualification is only slightly below the OECD average (OECD, 2019g). In addition, ICT specialists are poorly allocated, with over half of ICT graduates working in a field other than ICT, a share in line with Finland and Lithuania but higher than in Sweden, Estonia and Denmark (OECD, 2018e). This leaves Latvia with the lowest share of employees working as ICT specialists in the European Union, with the female share of ICT specialists halving from 30% in 2008 to 14% in 2018, driven by a fall in the absolute numbers of female ICT specialists (while the total number of ICT specialists rose) (Eurostat, 2019b). However, only 45% of firms that posted vacancies for ICT specialists encountered difficulties in filling these rolls, indicating easier hiring conditions than in most European OECD countries (Eurostat, 2020b). This suggests that the main driver of the lack of digitalisation among firms is the absence of incentives and a lack of workers with basic computer skills, rather than a lack of ICT specialists.

Figure 4.21. Firms finding it difficult to hire ICT specialists in Latvia and selected OECD countries, 2019

As a percentage of all firms posting vacancies for jobs requiring ICT specialist skills



Source: Eurostat (2020b), *Hard-to-fill ICT Vacancies: An Increasing Challenge*, *https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20200221-1* (accessed in February 2020).

Latvia also lacks the general skills necessary for the digital transformation (Box 4.4). Globally, greater use of ICTs has increased demand for generic and specialist ICT skills, as well as complementary skills such as online marketing and big data analysis (OECD, 2016a). Latvia has made large strides in raising educational attainment, with the share of 25-34 year-olds with a tertiary degree rising from 25% in 2007 to 42% in 2017, close the gap with the OECD average. Demand for graduates is evident from their higher earnings and employment prospects (OECD, 2018d). However, despite these gains, a large share of workers report being under-skilled for their job, while over-skilling is low and problems with quality of education remain, as evidenced by the mediocre literacy and numeracy skills of teenagers (OECD, 2019h; 2017a). In addition, there is a shortage of complementary skills, such as administration and management (Figure 4.19). Finally, low participation in life-long learning and a lack of in-work training hampers Latvia's efforts to adjust to the changing needs of the economy and to upskill those with low educational attainment.

Box 4.4. The digital transformation requires a broad mix of skills

In order to benefit from digitalisation, countries and their inhabitants need a broad range of skills, both to make effective use of the Internet, and to ensure they are not be left behind by changes in the labour market. This need for cognitive, socio-emotional and digital skills is the focus of the *OECD Skills Outlook 2019: Thriving in a Digital World* (OECD, 2019a).

Better literacy, numeracy and problem-solving skills are becoming essential for making effective use of the Internet and determining the reliability of online information. In addition, socio-emotional skills are a necessary aid for parents seeking to help their children confront issues such as cyberbullying. Conversely, lack of skills is an important factor that helps explain why some people do not access the Internet from their home.

A broad mix of skills is also necessary in the workplace as demand for skills changes. Technology is developing at an accelerating pace, creating new jobs while destroying others. Routine low-skilled tasks are being completed increasingly by new technologies, while demand grows for workers to undertake non-routine, cognitive tasks. It is therefore necessary for countries to ensure that training polices are in place to help workers adapt and find higher quality jobs. Such life-long learning can be assisted by improving the accessibility and quality of training at all stages in life.

Steps taken to improve digital skills

The demand for skills, such as those of ICT specialists, is likely to increase as firms embrace the digital transformation. Latvia has been taking steps to improve the skills of its workforce: the Information Society Guidelines aim to increase the ability of individuals to take advantage of opportunities offered by digitalisation; develop the skills of individuals, entrepreneurs and those in the public sector; train ICT specialists with the skills needed in the labour market; and introduce algorithms and digital literacy into school curricula. In order to achieve these aims, Latvia has been reforming its education and training system.

As it is not possible to predict with accuracy what skills will be required in the future, it is important that Latvia's inhabitants have the opportunity to update their skills throughout their working life (on the basis of a good general education in early life). In addition, they must be able to access continuing education in order to maintain and update their skills. Moreover, education and training institutions must be responsive to changes in demand for skills, as covered in the recent publication *OECD Skills Strategy Latvia: Assessment and Recommendations* (OECD, 2019i).

Latvia is gradually rolling out a revised general education curriculum (from pre-school to secondary education), moving from a knowledge-based curriculum to one grounded in competencies, through the ESF-funded "Competency Approach to Education Curriculum" project (more popularly known as Skola 2030) (MoES, 2020; VISC, 2019). The new curriculum aims to develop digital literacy as a transversal skill across all study areas, with the basics of coding taught from primary school onwards. In addition, computing will be taught in primary school from grade 4 onwards. The new general education curriculum is being gradually implemented as of September 2019 in pre-schools and September 2020 in primary and secondary schools (beginning with grades 1, 4, 7 and 10). The curriculum highlights the importance of developing digital and media literacy and ICT skills among students, and facilitating the use of ICTs as teaching aids (OECD, 2017a).

In addition, secondary school students pursue the ICT-related subjects "Computing" and "Design and Technologies", learning about topics including computer algorithms, languages and networks, and image, video and audio-processing, among others. Students have the option to continue with these subjects, or to study other topics such as coding, digital design or robotics at a more advanced level.

The digital transformation can also bring new challenges, such as cyberbullying, as noted above. Several organisations serve in the frontline to protect children from new digital threats in Latvia. For example, a phone line exists for children to report cyberbullying, while the "Superheroes on the Internet" collaboration between Net-Safe Latvia and the police promotes online child safety (Burns and Gottschalk, 2019). While Latvia is addressing such topics through the new curriculum, there is a risk that advice will become outdated as technologies change. Therefore, the MoES should consult with a wider group of stakeholders, such as the Latvia's Safer Internet Centre (Latvijas Drošāka Interneta Centrs), on a regular basis, to obtain advice on updating the curriculum.

In order to encourage an interest in ICTs among students and persuade them to pursue a career in ICT, Accenture Riga, Riga Technical University and MAK IT have formed the Start(it) Foundation. The foundation collaborates with Latvia's National Centre for Education to offer teaching aids and learning materials via an online portal (Startit.lv), as well as training for teachers. Over 400 teachers use their materials in over 300 schools, with over 15 000 people accessing the portal.

Adequate training of teachers is essential to ensuring the success of curriculum reforms and improving on previous outcomes. As in most OECD countries, Latvian schools that used ICTs most had the worst outcomes for reading, maths and science, reflecting the need for greater training of teachers (OECD, 2019a). Although a relatively high share (three-quarters) of teachers have had training in the use of ICTs as part of recent professional development activities, only half feel well prepared for the use ICTs in teaching. Although this is trend in line with the OECD average, further progress is needed to improve performance (OECD, 2019j).

Initial teacher training programmes have undergone reform to coincide with ongoing changes to the general education system. In addition, a new one-year study programme has been introduced for those who already hold a tertiary degree (e.g. in STEM subjects). The new programme includes development of ICT skills, and modules on using ICT in the learning process and developing digital content, among

others. Attracting STEM and ICT specialists to the teaching profession at secondary level may prove difficult. Teacher salaries in Latvia are low and have a flat wage structure, although school heads have some flexibility to raise a teacher's salary within the limits of the overall salary budget for the school (OECD, 2019i). Therefore, it may be necessary to pay teachers with STEM qualifications an additional allowance from national resources.

Vocational education is being reformed

Vocational secondary schools also offer training as ICT specialists for occupations including computer programming and systems technicians, among others. Vocational education is currently being reformed through the introduction of modular programmes. Modular updates allow schools to avoid a complete overhaul of the programme while giving students greater flexibility to follow topics in line with their interests. In addition, all modular programmes include a mandatory ICT component, which may be integrated into other modules. Finally, Latvia has established professional qualification requirements to align with the European Qualifications Framework (EQF) (OECD, 2019k).

Latvian vocational education and training (VET) has undergone modernisation, becoming less centralised with an increase in collaboration between local employers and VET schools, while the number of VET institutions has decreased as a result of consolidation. However, VET faces challenges such as high dropout rates, and institutions experience difficulty in attracting talented students. Greater use of career guidance for parents and students could help increase take up of vocational education. The EU-funded Effective Management for VET Schools (SO 8.5.3.) programme should be mainstreamed as a national programme (financed through national sources) when EU funding ends, as the initiative raises standards in VET schools. Meanwhile, co-funding Sector Expert Councils (SECs) could help raise the market relevance of VET (OECD, 2019i).

However, links between VET schools and firms could be improved. Latvia should increase the proportion of time students spend in work-based learning, which could help foster close links between schools and employers, and enable schools to adjust rapidly to the changing needs of employers – an issue of particularly importance for the rapidly changing skill requirements of ICT specialists. Indeed, several ICT-related firms in Latvia have demonstrated a willingness to play an active role in Latvia's education and training system. Although firms can receive a subsidy for the salaries paid to students participating in work-based learning, the administrative burden involved is high, and the subsidy is only available to firms without a tax debt. Latvia should therefore simplify the procedures to claim this incentive (OECD, 2019i). In addition, the provision of work-based courses in schools should be consolidated with direct links to employers.

Employer representation at the school level could also be further enhanced. Since 2016, all vocational schools include representatives of local employers on collegial advisory bodies, which support strategic governance. In addition, Vocational Education Competence Centres (VECCs) are responsible for approving new modules (OECD, 2019k). However, although SECs give employers a say in VEC curricula, such councils are not very representative (OECD, 2019c). Latvia could therefore increase the proportion of the curriculum determined at the school level. For example, in Slovenia, 15% of the content of programmes is decided by schools in co-operation with local companies (in addition to 25% of course time being devoted to work-based learning) (OECD, 2017b).

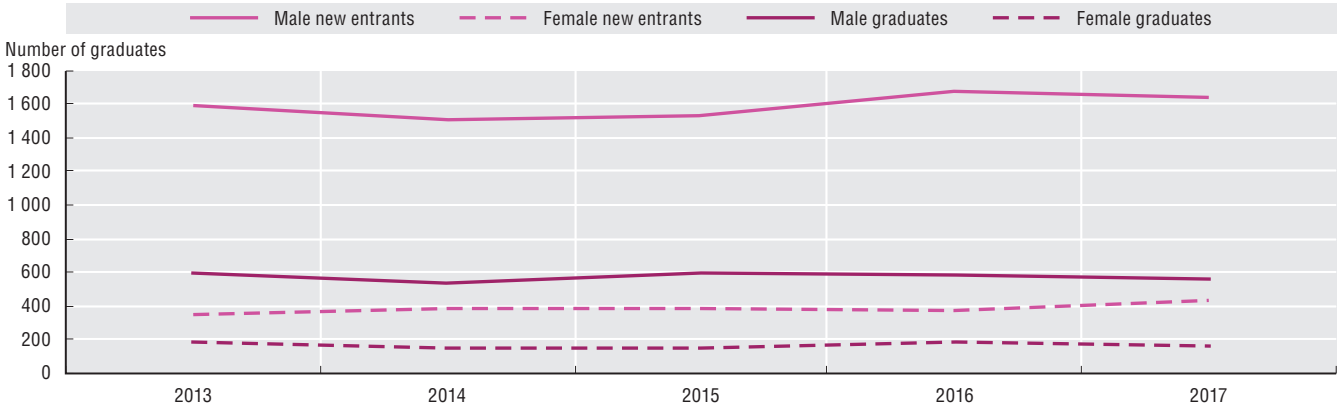
Latvia could also experiment with apprenticeships in ICT-related occupations – an approach already in use in other countries. For example, Austria, which has a well-developed system of dual education, introduced a three-year e-commerce merchant apprenticeship programme in 2018, to fill roles such as e-commerce manager in firms (WKO, 2018). The main incentive for firms to provide work-based learning (through apprenticeship programmes or in association with VET schools) should be the opportunity to access needed skills, rather than financial inducements. Latvia should therefore ensure a reduced administrative burden on participating firms and a high standard of training to enable apprentices to be productive. The government and/or social partners should also offer support or training to participating firms to help them design work practices that maximise learning. In addition, the government should monitor the training provided to ensure apprentices benefit from the programme (OECD, 2018f).

Higher education institutions are not increasing the numbers of ICT graduates

Latvian higher education institutions (HEIs) provide both professional and academic higher education, and accept students based on national centralised exam results (OECD, 2019e). A large number of HEIs are spread across the country producing positive effects on tertiary attainments (European Commission, 2018b). Public and private HEIs co-exist, though private ones tend not to offer STEM courses (OECD, 2019k). A slightly below OECD average (22%) proportion of graduates study in STEM fields, lower than in other Baltic countries. However, only 3% of Latvia's graduates aged 25-64 are in ICT fields, below the OECD average (though 5% of doctoral graduates are in ICT fields, above the OECD average) (OECD, 2019g; 2019c).

Latvia has introduced policies to increase the number of STEM and ICT graduates. The government has shifted public scholarships from social science to STEM, with a target of 27% of funding for scholarships in STEM fields by the end of 2020 (OECD, 2019k, 2019c). This move has led to an increase in the number of people studying STEM subjects, with the proportion of new graduates with a degree in ICT rising to 5% in 2017 (from 4.4% in 2015) – the seventh highest in the European Union (Eurostat, 2020c). However, the absolute number of students graduating from ICT courses has not increased, due to the high number of dropouts (Figure 4.22) (OECD, 2019k). In addition, Latvia has been unable to find suitable applicants to receive all the STEM scholarships offered, a consequence in part of the shrunken youth population.

Figure 4.22. Total number of tertiary ICT graduates in Latvia, 2013-17



Note: New entrants comprise the total new entrants to tertiary programmes, from short-cycle tertiary education to doctorate level.

Source: Eurostat, Education administrative data from 2013 onwards.

Latvia's higher education sector is currently modernising 300 STEM programmes, including ICT programmes. About EUR 70 000 will be spent on using ICTs to facilitate learning. The infrastructure used in ICT study programmes will also be modernised (including for 4 vocational programmes, 13 bachelor-level programmes, 13 master-level programmes and 7 doctoral programmes). The government also wishes to decrease fragmentation among study programmes (OP's SO 8.2.1), and 14 HEIs are implementing European Social Fund (ESF)-funded projects to develop 5 ICT study programmes, including programmes in languages other than Latvian.

Developing links between firms and HEIs can help improve the flow of information to HEIs regarding in-demand skills. Latvia has made progress in improving such links through programmes to boost innovation and research and development (see Chapter 6). In addition, some firms provide scholarships and offer traineeships to academic staff and students (Finance Latvia Association, 2019). Overall, however, links between HEIs and firms are not widespread and external stakeholders are not represented on university boards, making them less responsive to the changing economy (OECD, 2019i) (European Commission, 2018b). Building on existing links will help maintain the relevance of ICT programmes. This can be achieved by allowing employers to participate in course design and motivating a larger proportion of students to choose work placements. In addition, Latvia should introduce a legal framework for work-based learning in tertiary education (OECD, 2019i).

In addition, greater support for modular programmes combining ICT modules with other subjects (e.g. business) can help disseminate ICT skills across a wider range of Latvia's graduates. To this end, Riga Technical University (RTU) and Riga Business School, and the University of Latvia (LU), in

association with the Finance Latvia Association (an industry body) and Accenture, have established a bachelor degree programme entitled "Computer Science and Organisational Technologies".

Increasing students' knowledge of course outcomes can help them select the most appropriate course, and drive up standards. In order to improve quality assurance of Latvian education, in 2018 the Quality Agency for Higher Education (AIKA) joined the European Quality Assurance Register for Higher Education (EQAR) for a period of five years (OECD, 2019l). ICTs could also be used to improve students' knowledge of employment prospects. Since 2017, the MoES has been tracking graduate outcomes including data on graduate employment status, field of work, salary, and information about the institution and study programme that students decided to attend. The Ministry plans to make the data publicly available (OECD, 2019i).

A number of programmes also encourage women to pursue careers in ICT. In 2016, Riga Tech Girls was founded to encourage girls and women to develop digital skills, increase the visibility of women in the ICT sector, and establish a professional network of women in the ICT sector.

Unemployed workers have access to digital training

Traditionally, Latvia has offered limited social protection and spent below average on active labour market policies (ALMPs) (OECD, 2019k; 2019c). In recent years, however, the country has worked to improve its training system for unemployed workers, and labour market activation has shifted from providing jobs in the public sector to employment incentives and rehabilitation of the long-term unemployed (OECD, 2019k).

Latvia uses a system of training vouchers to provide training opportunities to jobseekers. The State Employment Agency (SEA) profiles ALMP participants based on self-reported information about the unemployed person and an interview with a caseworker. A SEA website then provides job seekers looking for training with information on competing training providers (e.g. the job finding rates of past participants) and labour market forecasts by occupation. Both formal training leading to accredited skills and more basic, informal training are provided. Informal training tends to last 42 days on average, compared to 91 days for formal training. Those lacking the ICT skills necessary to use the system are referred for informal ICT training. In 2018, over 18 000 people participated in the programme, with about 14 000 undertaking informal training, boosting their chances of finding a job (OECD, 2019k).

Informal IT training has been a popular choice for participants, with a 40-hour training course available for those with no ICT skills. In 2016, the most attended informal courses were basic IT (1 400 participants rising to 2 000 in 2017) followed by advanced IT skills (1 200 participants). In contrast, from 2012 to 2017 only about 1 000 people undertook formal training in ICT (compared to over 3 600 for formal training for welders) (OECD, 2019k). The SEA also provides ten digital skills upskilling programmes that last for 120 to 150 hours, as well as two vocational training ICT programmes. Short-term courses for older workers are also available and the SEA provides e-learning. The SEA meets annually with employers to ensure its courses meet the evolving needs of the labour market.

Latvia participates in the regional project Young ICT Women (No. 2017-1-094) which aims to teach digital skills to young women (ages 15-29) who are at risk of being excluded from the labour market. The Latvian operation is co-ordinated by LIKTA (with funding from the European Economic Area and Norway Grants Fund for Youth Employment) and will run from September 2018 to August 2021 (LIKTA, 2019; 2018). However, the programme is small (with the aim of reaching 700 women across seven countries). In addition, it is difficult to see how lessons learned could be transmitted to the SEA.

Greater use could be made of collected data

Latvia has its disposal a rich source of data comprising information from the SEA, the Social Insurance Agency, the Population Registry and the Social Assistance Database (OECD, 2019k). The SEA uses this information to produce a short-term labour market skills forecast (while the MoE produces a medium to short-term forecast.) A raining commission (*apmācību komisija*) uses these reports as a basis for setting fields of study for unemployed workers each year. Latvia's Digital Agenda and e-Government Strategy could make greater use of online tools for jobseekers at low risk of long-term unemployment, while web-scraping could help them find vacancies that are not registered with the SEA. In addition, data could be used to better monitor the effects of ALMPs (OECD, 2019k).

Although the Latvian State Education Information System (VIIS) collects data on education programmes, institutions and staff from early childhood education and care to higher education, certain data (e.g. characteristics of school staff) are in some cases unreliable. In addition, data on non-formal education and training and professional qualifications granted by non-public institutions are not collected, and electronic records of the qualifications people attained in the past are not available. To improve this situation, the Ministry is modifying the VIIS by linking it with higher education graduate tracking data and adult learning data (OECD, 2019i). The VIIS, the Unemployment Accounting and Registered Vacancy Information System (BURVIS) and the information system for the ESF project Improvement of Professional Competence of Employed Persons could also benefit from better linkages. In addition, data matching techniques could help create a more comprehensive picture of life-long learning (OECD, 2019i).

Firms lag behind in providing in-work training

Latvian firms invest relatively little in the skills of their workers, especially with regard to ICT training. Relatively few firms assess their future skills needs, and EEA enterprises are unwilling to invest in training due to the risk of trained employees moving abroad to obtain higher wages (VARAM, 2013). In addition, participation in life-long learning is very limited, with low-skilled workers less likely to take part in adult education (OECD, 2019c; 2017a). This is particularly stark in the case of provision of ICT training, with even larger firms lagging behind (Figure 4.23).

Figure 4.23. Businesses providing ICT training to their employees in Latvia and selected OECD countries, 2012 and 2018

As a percentage of all firms in each size group

Notes: Data refer to businesses with ten or more employees that provided any type of training intended to develop the ICT-related skills of their employees within the last 12 months. Data for New Zealand refer to 2016 and Iceland to 2014. Data for medium-sized firms in Portugal refer to 2017. Small firms have up to 49 persons employed, medium firms 50 to 249 persons employed, and large firms 250 or more persons employed.

Source: OECD (2017c), *ICT Access and Use by Businesses* (database), *http://oe.cd/bus*.

Latvia has two main ERDF programmes that support digital training for firms: "Technology training" (action number 1.2.2.1), which provides financing for ten industry associations to train ICT specialists; and "Non-technology training" (action number 1.2.2.3), which includes training in the use of ICTs. These programmes are implemented by industry associations, such as LIKTA. In addition, the more generally oriented ESF-funded project Developing Professional Competencies of Employees (SO 8.4.1) aims to improve, among others, the ICT proficiency of adult employees with low skills.

The project Training of ICT Professionals to Promote Innovation and Industry Development (no. 1.2.2.1/16/A/003) has been designed to raise the skills of ICT professionals and help overcome the shortage of such individuals within Latvia. The project was run by LIKTA, and trained 1 630 ICT professionals from 77 firms up to March 2019 at a cost of EUR 1.8 million (with EUR 900 000 financed by the European Union) (EsFondi.lv, n.d.).

In order to provide ICT training to self-employed workers and staff in micro and small firms across several of Latvia's regions, LIKTA initiated the project For the Development of Innovation and Digital Technology Training for Small and Micro Business Operators in Latvia (no. 1.2.2.3/16/I/002), running from December 2016 to December 2020. Businesses are evaluated to ascertain their needs and the tasks of their employees, and then appropriate training is recommended, which covers topics such as data security, digital marketing and digital tools for customer service, among others. Participants that complete the training receive a certificate. The aim is to train 6 500 participants at a total cost of EUR 2.7 million (70% funded by the ERDF) (EsFondi.lv, 2015).

Box 4.5. Changing the education and training system to keep up with a changing economy

Adapting Latvia's education and training system is crucial to meeting the needs of a changing economy and society. With this in mind, Latvia is developing a National Medium-term Strategy for Education and Skills (2021-2027). This strategy is the main focus of *OECD Skills Strategy Latvia: Assessment and Recommendations* (OECD, 2019i), which examines all stages of Latvia's education and training system, from early childhood to tertiary education, and onward to continuing adult education, with a focus on improving the skills of students, fostering life-long learning, reducing skills imbalances and improving governance of the skills system.

The report finds that an adaptable workforce is necessary for Latvia to take advantage of the opportunities offered by the digital transformation. Highly qualified teachers can help students achieve the foundational literacy and numeracy skills early in life that will allow them to be more adaptable in later life. Latvia should continue to develop the skills of Latvia's aging teachers (i.e. by linking teacher appraisal with continuing professional development), and assess and evaluate schools to ensure accountability.

Fostering a culture of life-long learning can also help adults keep pace with a changing economy. This can be achieved by increasing awareness of opportunities to participate in life-long learning and reducing barriers to participation, while increasing provision and quality. In addition, Latvia should move beyond reliance on European Structural Funds for adult education to seek a broader spectrum of funding sources, and VET schools should increase the training offered to adult learners.

The education and training system itself must also respond to changing needs. The tertiary education system could improve its level of responsiveness by increasing collaborations between HEIs and employers, such as through work-based learning. In addition, governance of education and training could be more responsive to changing demand, for example by creating partnerships with social partners to draft skills policies.

Finally, the responsiveness of the labour market could be enhanced by easing the migration of skilled workers from abroad and facilitating mobility within Latvia.

In addition, the Latvian Chamber of Commerce and Industry (LCCI) is implementing a project entitled "Productivity Evolution 2" (no. 1.2.2.3/16/I/001), which focuses on raising productivity in small firms across a wide range of sectors. Training covers areas such as accounting and hotel management, and can include the use of ICTs. The project aims to train over 4 700 people in 285 firms by the end of 2020 (LCCI, 2017), and as of November 2019, over 1 850 employees and 199 firms had participated at a total cost of EUR 1.7 million (with EUR 900 000 provided by the ERDF) (LCCI, 2019).

Employers are hesitant to pay for training for their workers for fear of losing them to other firms, with Latvia performing poorly overall in terms of funding of adult education (OECD, 2019m; 2019i). Latvia should therefore create a shared training fund, and charge employers a training levy (as a percentage of gross wages). Firms can then draw from this fund to pay for non-firm specific training (including training to use new digital tools), or be refunded the levy in the form of training vouchers. Such levy-grant systems currently operate in France, Italy and Poland (among others) (OECD, 2019m). As workers can face obstacles to participating in training, such as financial barriers or family responsibilities, the fund could also cover part of a worker's salary during the training period (OECD, 2019n).

Easing migration and accessing the skills of foreign ICT workers

Latvia's skill shortages are exacerbated by policies that hamper the return migration and immigration of skilled workers. In particular, strict Latvian language requirements for many professions can discourage the return migration of Latvians with a foreign spouse (OECD, 2016b). Although Latvia is becoming a popular destination for foreign students, only a small number stay after graduation, though the government aims to increase this proportion to 10% by 2030 (OECD, 2017a). In addition, the government recently took action to ease labour market tests for shortage occupations (OECD, 2019c). The minimum necessary salary to be offered to a foreign worker has been reduced from 50% above the average wage to 20%, and the number of days the position must be registered with the SEA as vacant has been reduced from 30 days to 10. Given the high demand for ICT specialists, Latvia should abolish labour market tests for those able to prove experience working in the field or an appropriate qualification, as is the case in Germany and the United Kingdom (Box 4.6). In addition, removing labour market tests for individuals that have completed their studies in Latvia would help ease skill shortages (OECD, 2019c). Finally, a tax credit for student loans could be particularly attractive for those that studied abroad and would help attract workers with much-needed skills.

Box 4.6. Germany and the United Kingdom use simplified procedures to hire ICT specialists from abroad

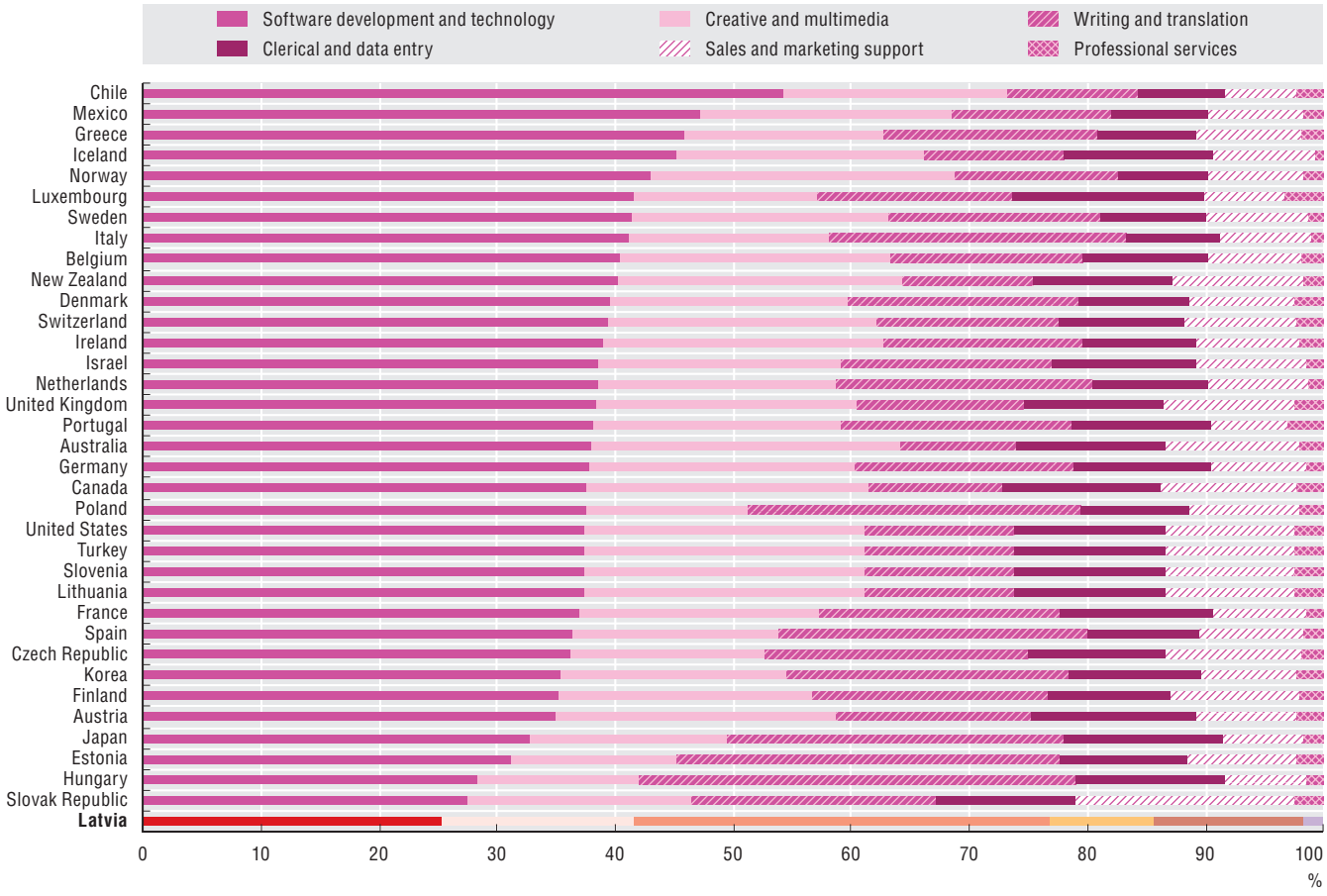
Germany's new Skilled Immigration Act has simplified the hiring of skilled migrants from outside the European Union, in particular ICT specialists. Workers from outside the European Union with an appropriate qualification and a level of proficiency in the German language no longer need to have a work contract to reside in Germany, but can instead obtain a six-month residence permit allowing them time to find a job. ICT specialists do not need evidence of an appropriate qualification if they can prove that they have worked in the role for several years. In addition, employers no longer have to show that they were unable to find such expertise within the European Union (Zech, 2020).

The United Kingdom has also simplified procedures for hiring ICT specialists from abroad. Those applying for a job included on the Shortage Occupation List (which includes ICT specialists) do not need to meet the requirement of a minimum salary of GBP 30 000, allowing less experienced workers to find a job within the field. As in Germany, employers no longer have to pass the Resident Labour Market Test to prove that they were unable to find a suitable worker within the European Union (gov.uk, 2020).

Use of freelance workers also gives firms access to an extended workforce. In particular, greater use could be made of online labour, as Latvia is unusual in terms of the low proportion of software development and technology tasks in online labour markets, with writing and translation having greater importance (Figure 4.24) (OECD, 2019a).

Figure 4.24. Online hiring by occupational group in Latvia and selected OECD countries, 2018

As a percentage of all projects/tasks posted on online platform by country of employer



Notes: Each bar displays employer countries' share of projects/tasks posted on online labour platforms between January and July 2018, by the occupation of project/task. For example, for projects/tasks posted online by employers based in Chile, over 50% of these were related to software development and technology, and 20% to creative and multimedia. The Online Labour Index tracks all projects and tasks posted on the five largest English-language platforms, which account for at least 70% of all traffic to online labour platforms. The occupation classification builds on that used by Upwork.com.

Source: Kässi and Lehdonvirta (2018), *Online Labour Index: Measuring the Online Gig Economy for Policy and Research*, *https://mpra.ub.uni-muenchen.de/86627* (accessed on 20 June 2018).

Usage by business: Conclusion

Latvian firms have advanced in their use of digital technologies, but still lag behind other OECD countries. While boosting the digital skills of the Latvian workforce will be necessary to help firms adopt digital technologies, there is currently a lack of incentives for firms to adopt such technologies. The recommendations in this section to boost the uptake of digital technologies and improve digital skills are summarised in Box 4.10.

While firms are an important driver of the digital transformation, use by government also plays a key role. This is discussed in the following section.

Usage of digital technologies by the government

Adoptions of ICTs by the government sector can act as a powerful driver of adoption by firms and households. In Latvia, increasing the use of digital technologies and data by government is an important component of the Information Society Development Guidelines. Use of online services and e-health, as an alternative to face-to-face consultations, can also help Latvia address some of the challenges created by the COVID-19 pandemic. In line with the digital government strategy, Latvia has made strong

advances in the delivery of online services and provision of open data, becoming one of the leading countries for digital government in the European Union (European Commission, 2019b). Nevertheless, to date Latvia has focused largely on improving the efficiency of public services and has yet to take full advantage of the ability of digital technologies to change how services are designed and to use data to improve policy making.

Current strategy for use of ICTs by government

Latvia's strategy for digital government is presented in the Information Society Development Guidelines, with further details added in the Concept for Improvement of the Public Service System (January 2015) and the Public Administration Reform Action Plan 2017-2020. In part, the strategy was driven by the need to increase efficiency in the public sector due to budget constraints following the international financial crisis. The Information Society Development Guidelines focus mostly on plans to improve internal processes in the public sector, and the delivery of services digitally, although mention is made of the use of ICTs to redesign processes (Box 4.7).

Box 4.7. Latvian's Information Society Development Guidelines

The Information Society Development Guidelines include two sets of Action Directions related to increasing the use of ICTs in government.

The following actions are included under **advanced and effective public administration**:

- modernisation of basic public administration processes
  - transformation and optimisation of basic processed
  - digitalisation of basic operational processes
  - digitalisation of support processes
  - collaboration between public administration processes
- public e-participation and e-democracy
- single public administration data space
- optimisation of ICT infrastructure.

The following actions are included under e-services and digital content for public:

- opening of public administration data and transaction services to other users
- shared platforms and service development for provision of public services
- provision of official e-mail addresses to inhabitants and entrepreneurs
- digitalisation of public services
- automated issuing and acceptance of electronic invoices
- digitalisation and accessibility of cultural heritage
- stimulation of Latvian language usage in the digital environment
- e-health solutions for efficient, safe and patient-oriented health care.

The strategy links with the Latvia as a Data Driven Nation framework, which aims to build a society that makes intensive use of data generated in the public and private sectors. The plan was approved by the Information Society Council and consists of three pillars: 1) data democracy and accessibility; and 2) data-enabled citizen engagement; and 3) data-driven innovations/innovative data commercialisation.

The Ministry of Environmental Protection and Regional Development (VARAM) is the lead ministry for digital government policy. The State Regional Development Agency (VRAA) forms part of VARAM and operates centralised services (e.g. the citizen portal Latvija.lv, the data exchange platform VISS.gov.lv and e-payments) for municipalities and state agencies. The VARAM monitors all digital government projects funded by the ERDF, ensuring their compliance with government ICT architecture.

However, Latvia faces some challenges in implementing its strategy, notably the lack of a co-ordinated ICT procurement strategy, with ministries instead making their own decisions. Although VARAM is exploring ways to improve services for citizens (including scenarios that involve interacting with different agencies, such as when someone is establishing a firm), the Ministry lacks the power to make decisions mandatory. In addition, staff may lack the necessary skills, while some agencies may not consider digitalising services to be a priority. Consolidating funding for digital government into a single ministry, such as VARAM, which also has responsibility for developing the digital government strategy, could help ensure more streamlined delivery of the government's digital government strategy (see Chapter 7). Alternatively, co-ordinating mechanisms (e.g. a representative committee to co-ordinate digitalisation) combined with policy levers (e.g. budget thresholds or funding mechanisms) could help improve co-ordination.

In addition, Latvia lacks a civil service-wide training strategy. Training in IT and digital skills is not currently considered a priority for civil servants, although online learning is available (OECD, 2019o). Such a strategy should include training in the use of ICT, as well as in the design of services to ensure ease of use for service users. In addition, greater progress could be made in sharing lessons learned from digitalisation across the public sector by developing a manual of good service delivery practices. This could constitute a first step in the creation of a civil service culture to promote the digital transformation. The United Kingdom has already created such a manual which includes a 14-point service standard that public services must meet, including technical requirements and design standards to ensure ease of use by the public, and ways of measuring success such as web analytics (Government Digital Service, 2019).

Colombia has dealt with some of these challenges through its Online Government Excellence Programme (*Programa para la Excelencia en Gobierno Electrónico*), which aims to promote an innovation culture within public sector management. The programme includes workshops and virtual courses for public servants, in addition to graduate and postgraduate training. Such a centralised programme can help create a community of digitalisation experts, and help apply lessons across the public service. In addition, Colombia offers a Seal of Excellence (*Sello de Excelencia*) for online government services and procedures that reach a high standard. This helps to raise awareness of successful digitalisation projects within the public sector.

Progress in digitalising services

In July 2017, the Latvian government introduced new regulations (Cabinet of Ministers Regulation No. 402) for the digitalising of public services. Where feasible (and taking into account cost-effectiveness), public entities must provide a service electronically if the service is requested 5 000 times within a year, or if it accounts for at least 10% of all services provided by that entity. In addition, the service must be digitalised if it improves availability of the service and convenience for clients, and reduces the administrative burden or the costs of providing the service. The regulation also outlines the approach to be used to ensure that services are user friendly and service providers publish performance indicators (e.g. the proportion of attempts to use the service that are not completed). Service providers must ensure that accessing a service electronically is faster for recipients than the analogue alternative, or comes at a lower cost.

Latvia has digitalised services in many sectors in recent years. For example, the SEA has been using ICTs to improve services for the unemployed (see above), and the State Education Development Agency processes applications online for the education of employed adults. In 2018, Latvia also launched the Travel Safe (Ceļo droši) app to warn people of risks abroad and to advise them of courses of action in the event of an emergency (European Commission, 2019c). Government e-services can be accessed via the Latvija.lv portal, which provides information, consultation options and eProcedures (e.g. uploading of forms, fully automated electronic services and online payments) (European Commission, 2019c). Over 800 e-services are available to the public, with over 100 added in 2019. Almost 700 000 registered users made use of a service in 2019 (VRAA, 2019).

In April 2018, the government launched the My Latvija.lv! Do Digitally! (Mana Latvija.lv Dari Digitali!) campaign to encourage inhabitants to make use of available e-services. The campaign included training for 6 000 national and local government officials to help the general public use e-services. In addition, the government developed video tutorials on how to use the services and carried out an information

campaign via traditional and online media. From 2017 to 2019, the number of people registered with the national services portal increased by a quarter (to over 1 million), nearly doubling the share of users. These indicators suggest a successful campaign; however, the increase could be due to other factors. More granular performance indicators made possible by digital technologies could identify, for example, whether hits to websites increase in the days following an information campaign. Greater use of such web analytics could help ensure that resources are used in the most effective manner.

Digitalisation of services is being facilitated by the creation of electronic IDs, in conjunction with the establishment of a legal framework for mandatory electronic identification. These physical cards include biometric data that can be read electronically, allowing the holder's identity to be verified and enabling the creation of a valid electronic signature. They can be used as ID and travel documents. Although eIDs have been issued since 2012, from 2023 onwards having an eID will become mandatory (Office of Citizenship and Migration Affairs, 2020). In addition, a new app allows people to use a smart phone to authenticate their e-Identity and digitally sign contracts. The use of this app increased during the COVID-19 pandemic (eParaksts, 2020).

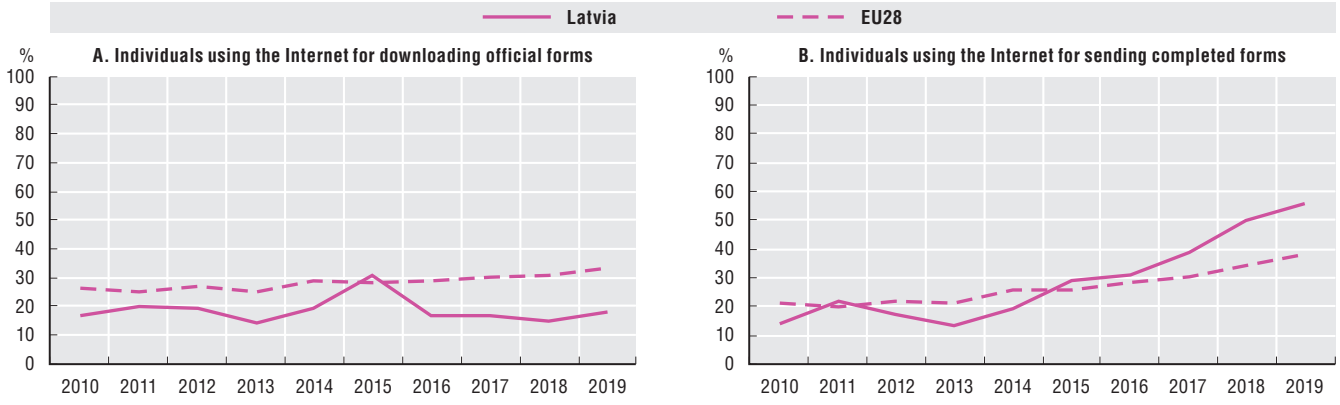
In addition, the Latvian government is moving to a "digital by default" principle for communicating with the population, although those without Internet access can opt out or make use of local Unified Customer Service Centres (see below). Official electronic addresses were introduced under the Official Electronic Address Act on 1 March 2018, in order to ensure secure communications between public bodies and individuals. As of June 2018, all public bodies have electronic addresses (from which point individuals may also get an electronic address) and 3 000 public entities have an obligation to only send documents electronically in response to an inquiry by the public. From 2020, businesses will also have electronic addresses (European Commission, 2019c).

Making services "online only" (as is the case with the state land support service) can act as a driver of adoption of digital technologies among firms and households. Latvia has ensured that digital-only services are accessible via Unified Customer Service Centres (see below), thus ensuring accessibility for those who do not use the Internet.

These measures have resulted in services becoming more user friendly. The proportion of people who only download official forms has fallen, with more people completing forms online (Figure 4.25). In addition, an above average proportion of users use the Internet to interact with public authorities (Figure 4.8).

Figure 4.25. Trends in the use of online services in the European Union, 2010-19

As a percentage of all individuals aged 16-74



Source: Eurostat (2020c), *ICT Usage in Households and by Individuals* (database), *https://ec.europa.eu/eurostat/cache/metadata/en/isoc_i_esms.htm*.

Digitalising business interactions with the state is also been a priority of the Business Environment Development Measures Plan 2017-2020 (Cross-sectoral Coordination Centre, 2017). Indeed, digital communication is mandatory in some sectors; for example, as of 2019, all documents related to the construction of new buildings must be submitted via an online portal. Latvia should create incentives for businesses to interact with government online, such as by prioritising businesses that access

services digitally (e.g. by issuing permits or payments more quickly to firms that interact online). In addition, Latvia should develop a schedule for which services to businesses are only delivered online.

Considerable progress has been made in digitalising health services

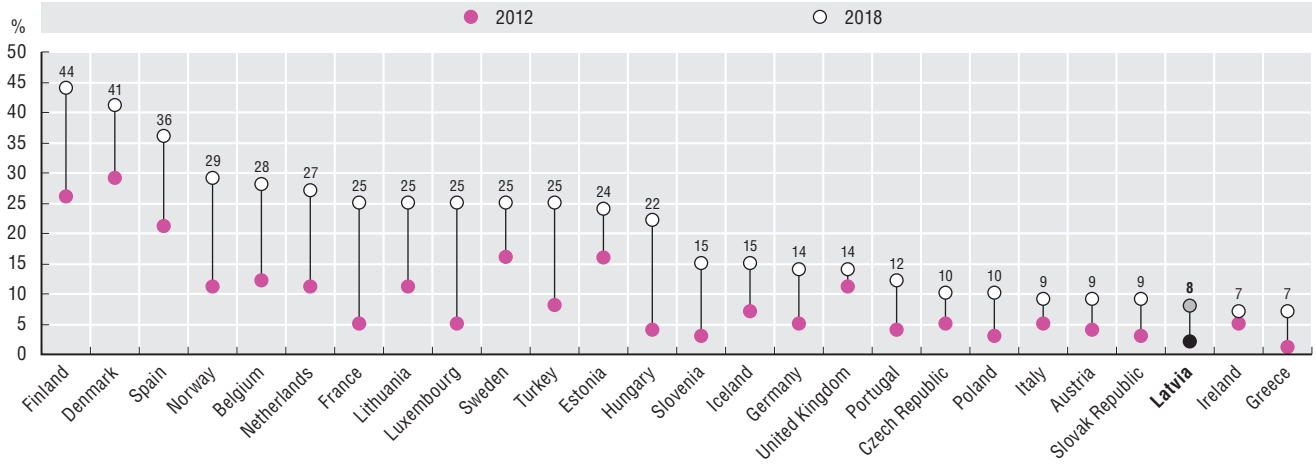
The goal of Latvia's e-health policy is to improve the efficiency of health care delivery by improving the sharing of information and reducing the time spent by medical practitioners on bureaucratic activities. The benefits of e-health have become even more apparent during the COVID-19 pandemic. The e-Health policy aims to enable individuals to more easily control their health care; reduce the time that patients waste in contacting medical institutions; make it easier for medical practitioners to access a patients records, while reducing duplication of entry; and increase the reliability and security of health care data. It is estimated that digitally transforming the health system could bring benefits equivalent to 8% of health expenditure (OECD, 2019p). Such benefits are likely to be large due to the size of Latvia's aging population and associated increases in health problems.

Since 2016, personal electronic health records have been available to patients and health professionals, albeit with some limitations (e.g. the absence of immunisation data). In addition, since 2018 e-prescriptions have become mandatory for state-reimbursed drugs, and sick leave certificates can only be issued electronically, with the system linked to social insurance payment of sickness benefit (European Commission, 2018a). Medical practitioners can electronically refer patients to a specialist or for a diagnostic test, prepare medical documents and view documents prepared by other health practitioners during a consultation, but may also deny a patient the right to view certain medical information. Patients can grant or refuse access to their information, although early problems regarding data privacy has dented confidence in the system among some of Latvia's population (European Commission, 2019c; Menshikov and Volkova, 2019).

However, a relatively low share of Internet users access health information online, with the proportion particularly low for men (Figure 4.8). In addition, the share of people who make medical appointments online is relatively low (Figure 4.26). Greater regulatory certainty regarding the privacy of health data could help foster the development of a booking platform for medical appointments, similar to the Doctolib platform used in France and Germany, the information gleaned from which could be useful in monitoring the health of Latvia's aging population. Greater use could also be made of data currently being collected, for example to predict flu epidemics and advise vulnerable people about vaccinations.

Figure 4.26. Individuals who made an appointment with a health practitioner on line in Latvia and selected OECD countries, 2012 and 2018

As a percentage of all individuals aged 16-74



Source: Eurostat (2020c), *ICT Usage in Households and by Individuals* (database), *https://ec.europa.eu/eurostat/cache/metadata/en/isoc_i_esms.htm*.

Further progress in health requires a national digital strategy, stronger governance of health data, greater institutional and operational capacity (e.g. by giving the workforce and the public the skills to make effective use of new systems), and clear laws regarding the privacy of health data. Finland, the

Czech Republic and Sweden shave all made good progress in meeting the requirements for the digital transformation of the health sector (Box 4.8) (OECD, 2019p). Latvia should ensure the interoperability of data and ICT systems within the health sector. In addition, the government should create clear policies to protect private data, and only link data from different data sources with the consent of patients (see Chapter 5). Finally, research using health data can be facilitated through the creation of a one-stop shop, possibly in association with an HEI, for those who wish to access health and social care data.

Box 4.8. Establishing clear rules is necessary to facilitate the sharing of medical data

The OECD *Recommendation of the Council on Health Data Governance* (OECD, 2016c) offers guidance to countries on how to manage the risks – and reap the rewards – of health data. It includes 12 principles, such as ensuring that individuals are aware of how their data are used, and making sure that individuals processing personal data receive training in privacy and data security.

Several countries have implemented strategies to regulate the sharing of health data.

Sweden's digital health strategy aims to increase data sharing between various public authorities and citizens while maintaining privacy and data security, and ensuring the interoperability of data and ICT systems within the health system. In Sweden, patients can access their electronic health records which include information on their vaccine history, test results and referrals, among others.

Meanwhile, Finland's My Kanta allows those with a Finnish personal identity code to access medical records, manage consents (for sharing data and organ donation) and to see how their data have been used. Only 4% of users in Finland have opted out of sharing their medical data for research purposes. In addition, Finland is creating a one-stop shop for those who wish to access health and social care data for research reasons, which will act as a single entity to approve the use of data (OECD, 2019p).

Finally, the Czech Republic is developing an Act on eHealth and Secure Data Sharing between HealthCare Providers, as the current, fragmented legislation makes effective management of the e-health system impossible. The goal is to establish core rules, procedures and standards, including safety for digitalisation of the health sector. In addition, the Act aims to define rules, competences and rights with regard to increasing patient involvement in the health care system.

Greater use of digital technologies can help Latvia face the challenge of an aging population, including increasing pressure on the health system, as evidenced recently by the need to cope with patients who may have a highly contagious illness, such as COVID-19. Latvia should therefore develop pilot programmes for telemedicine and pursue those with clear benefits, while facilitating the spread of best practice. Although telemedicine is permitted, legislation is not yet in place to govern its use (in contrast with Denmark, Finland and Poland) – including whether a patient must be physically present with a medical practitioner when a prescription is written. Denmark has experienced success with telemonitoring: the home monitoring of patients with chronic obstructive pulmonary disease has become mainstream following a randomised control trial, and another telemonitoring programme is being used for babies born pre-term. Video consultations are also being used (Oliveira Hashiguchi, 2020). As inequalities in digital literacy mean that those most likely to benefit from telemedicine are least able to take advantage, such policies should be combined with community-based initiatives to improve digital literacy.

The use of data and algorithms can be especially useful for supporting patients with complex needs, such as elderly individuals being treated with several medicines simultaneously (OECD, 2019p). The Nordic Council (Denmark, Finland, Iceland, Norway and Sweden) has created a Nordic Programme on Health and Welfare to strengthen research co-operation in these areas (OECD, 2019p). Creating a similar programme among the Baltic States could help pool resources to face common health and welfare challenges.

Use of ICTs to improve services

Latvia has gone beyond the digitisation of existing processes and is now in the early stage of using digital tools to change how services are delivered. The tax authority is using data to better target tax audits, while the SEA is using digital tools to assess the needs of the unemployed (see above). However, the government could capitalise further on the data collected through digitalisation to provide more targeted and personal services (Box 4.9).

Digitalisation has also allowed Latvia to change how it delivers services to the public. In 2011, the country adopted a "one-stop shop" principle to access public services, whether in person or digitally, and since 2014 a network of state and municipal Unified Customer Service Centres (VPVKAC) has been operational. These centres offer digitalised services from various bodies, such as the State Revenue Service (SRS) and SEA, available across 78 municipal centres. In total, over 800 government services have been digitalised. Although VARAM created the one-stop shop principle, individual agencies are responsible for delivering services. Individuals can use the "Less Burden" web-tool or the Futbols app (available only in Latvian) to rate services and submit proposals for improvements to services, which are then evaluated by the State Chancellery.

Latvia has also developed e-participation processes. In 2013, a petition website (manabalss.lv) was launched where any Latvian citizen aged 16 or over can propose and electronically sign an initiative. If an initiative receives 10 000 signatures, it is added to the agenda of Parliament. In December 2015, a regulation was passed allowing citizens to submit petitions electronically (if the submission includes a way to verify the electronic signatures) (European Commission, 2019c). However, only a relatively small proportion of the population use this tool to voice their opinions to public officials, and only 7% use the Internet to express their opinions online (OECD, 2019i; 2019q).

Latvia has also been making use of digital technologies to help overcome the language barrier for inhabitants that do not speak Latvian as their first language. The machine translation portal Hugo.lv enables English and Russian speakers to access Latvian language information and e-services. Latvia plans to supplement this service with the creation of a virtual assistant, to allow individuals to make use of e-services in their preferred language. In addition a company, Tilde, is researching translation technologies (NIFO, 2018).

Box 4.9. Promoting digitalisation in regional locations

Promoting digitalisation in regional locations is a priority for Nordic countries – and the topic of the Nordregio report *Governing the Digital Transition In Nordic Regions: The Human Element*, which found that regional digitalisation is a human rather than technical process (Randall and Berlina, 2019).

Helsingborg, in southern Sweden, stands out as successful example of embracing digitalisation. Under the Mayorship of Palle Lundberg, rather than developing a strategy to improve municipal work processes, the municipality emphasised experimenting and learning. In addition, the process focused on the needs of citizens rather than IT systems. Finally, digitalisation was considered the responsibility of all municipal employees and residents of the city.

On the basis of this approach, the city developed the platform My Helsingborg to access services and Smart Helsingborg to allow residents to create services. A space was also created for residents to borrow new technologies and experiment with them. As a result, in 2015 Helsingborg won an award for the best IT municipality in Sweden. This was followed in 2016 by an award for the leading e-commerce city in southern Sweden.

In this case, the key factor for success was long-term political support and leadership that encouraged experimentation and was willing to tolerate failures if lessons were learned.

The creation of an annual workshop involving both public servants and researchers, such as academics, where ministries demonstrate how they use data to improve decision making, could foster the sharing of ideas and expertise within the Latvian public sector. In addition, Latvia should support the creation of a social research unit, either within a state agency, or as part of an HEI, to analyse data and recommend new services. The unit would either have the competency to conduct such research in house, or would

outsource it to universities. In addition, the unit should have the ability to make anonymised micro-data available for approved research projects by outside organisations (taking into consideration privacy concerns).

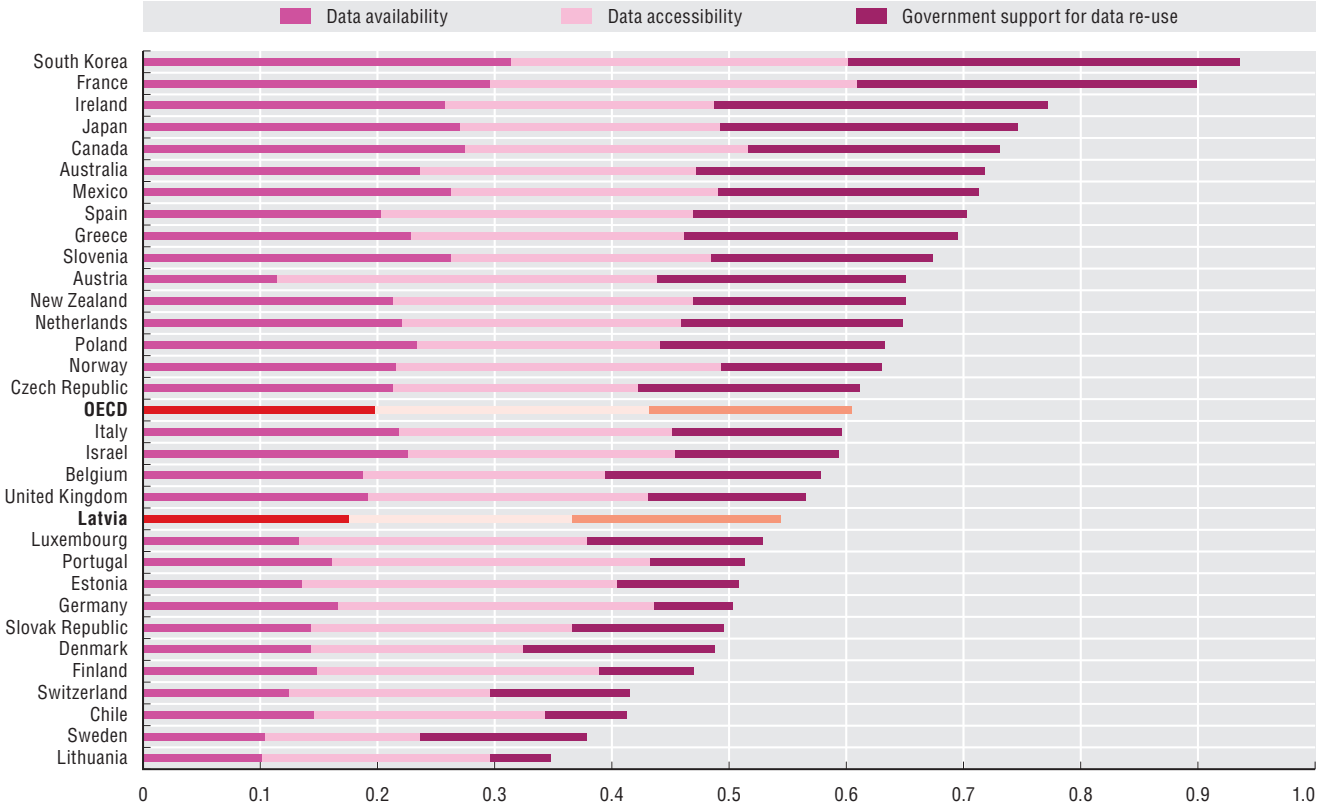
Latvia has made substantial progress in improving services, although further steps are needed to develop a data-driven public sector. Usage of data can help the government enhance planning of services and anticipate demand peaks, in addition to improving planning and monitoring. It can also help boost public trust in government. Such steps require a strong vision and leadership, coherent implementation, rules and guidelines for the use of data, as well as data infrastructure and architecture (OECD, 2019r).

More government data are now publicly available

Making government data publicly available can enable firms to develop new apps that make use of such data, allow researchers to investigate ways to improve public service delivery and heighten transparency, which in turn increases trust in government. At present, there is low trust in public institutions, with Latvia ranking below the OECD average in The World Bank's Worldwide Governance Indicators (WGI), performing poorly for Control of Corruption, and Voice and Accountability (OECD, 2019e; 2019k).

Increasing the openness of data has been a government priority and considerable progress has been made in this regard, with the government approving a new Open Data Strategy (Latvijas Atvērto Datu Stratēģija) in 2019 (Figure 4.27). The Information Society Guidelines (2014-2020) include a requirement that data must be available for use and re-use as part of their five criteria for state information systems. In addition, Latvia is making efforts to comply with the European Public Sector Information Directive. In July 2017, the government approved the Third Action Plan for Open Government Partnership. This includes plans to develop an open source public data portal, a research and publication database, and a database of state-owned capital companies. Latvia also plans to produce a portal for the circulation of draft legal acts, modernise the statistics portal and take measures to reduce red tape (*www.mazaksslogs.gov.lv*) (State Chancellery, 2017).

Figure 4.27. Open Useful Re-Usable data (OURdata) Index 2019



Source: OECD (2019o), *Government at a Glance 2019*, *https://dx.doi.org/10.1787/8ccf5c38-en*.

In 2017, the Latvian Open Data Portal was launched making available over 260 datasets. Public institutions publish data in a machine-readable format, together with metadata, in line with an order of the Cabinet of Ministers (European Commission, 2018a). Institutions are responsible for the published data but receive support from VARAM, while the State Regional Development Agency (VRAA) (an agency of VARAM) operates the portal. All the data are also available via the European Data Portal (European Commission, 2019c). However, efforts to make more data available ran into difficulties, as some of the most valuable data (e.g. geospatial address data) constitute a source of income for agencies.

As a result of these efforts, the availability of open data has increased considerably since 2014 (Table 4.1). Data on government spending and geospatial data (on postcodes and maps) have become freely available, while data previously freely available in a limited form (e.g. transport timetables, government budgets, election results and legislation) are now available in a machine-readable form under an open licence. This can facilitate the creation of apps and other digital tools, in line with Latvia's intention to create innovative services in the private sector through digital public administration. Openness can also have the benefit of increasing transparency and accountability and, thus, improving trust in public institutions.

Table 4.1. More government data has become publicly available

Change in openness of government data since 2014

	Data exists	Available digitally	Publicly available	Free of charge	Available online	Machine-readable	Available in bulk	Open license
Transport timetables	P	P	P	P	P	+	+	+
Government budget	P	P	P	P	P	+	P	+
Government spending	P	P	+	+	+	+	+	+
Election results	P	P	P	P	P	+	+	+
Company register	P	P	P	P	P	P	P	+
National maps	P	P	P	P	P	P	+	+
National statistics	P	P	P	P	P	P	+	+
Legislation	P	P	P	P	P	+	+	+
Postcodes/zip codes	+	+	+	+	+	+	U	+
Pollutant emissions	P	P	P	P	P	P	+	P

Note: "P" = previously available in 2014; "+" = added subsequently; "U" = unavailable.

Sources: Bojars and Liepins (2014), "The state of open data in Latvia: 2014"; questionnaire responses.

All open data are published under an open licence and are available free of charge. Latvia has made particular efforts to ensure the availability of valuable geospatial data. In part, the availability of open data has been driven by a seminar campaign which sought to inform ministries and their agencies of the importance of open data. This awareness-raising effort was accompanied in September 2018 by an open data "hackathon".

The government should do more to promote an open data ecosystem within Latvia. Alongside a social research unit (see above), Latvia could create a prize fund to award grants and prizes to tertiary-level students who make use of open data in their coursework, and give prizes to other researchers and software developers who use open public data to solve problems to the benefit of the public.

Using government procurement to promote the digital transformation

The government could make greater use of public procurement rules to encourage SMEs to adopt digital technologies. At present, public procurement accounts for a fifth of GDP. Latvia's electronic procurement system is managed by the State Regional Development Agency and can be used by municipalities and state agencies. In 2017, eCertificates, which provide information about suppliers, were added to the system to simplify procedures for firms. Since January 2019, all tenders must be submitted electronically for amounts over EUR 10 000 (European Commission, 2019c). In addition, the National Electronic Procurement system now uses standardised forms to reduce the administrative burden for firms. Latvia's e-procurement system is also integrated with the tax register (European Commission, 2018a) (OECD, 2018g; 2019o). The government should build on this infrastructure by

necessitating electronic invoices for procurement in a standardised machine-readable format (as is standard in Norway).

Although Latvia has a green public procurement plan, the government does not use public procurement to support innovation (European Commission, 2018b; OECD, 2019e). Creating a website to allow SMEs to find smaller value public contracts, such as the Contracts Finder website in the United Kingdom, could encourage Latvian SMEs to increase their use of digital technologies. Similarly, Colombia has created a Virtual Shop (*Tienda Virtual*) for firms that have signed a price framework agreement with Colombia's central procurement authority. This portal allows government entities (including municipalities) to directly purchase commonly bought items from firms. Creating a similar portal could act as a driver for smaller firms to engage in e-commerce.

Usage by the government: Conclusion

Increasing government use of digital technologies and data constitutes an important part of Latvia's Information Society Development Guidelines. The use of online services and e-health, as an alternative to face-to-face consultations, can also help Latvia address some of the challenges created by the COVID-19 pandemic. While Latvia has made strong advances in the delivery of online services and provision of open data, further steps are necessary to seize digital opportunities.

Conclusions and policy recommendations

Latvia has made considerable progress in the use of digital technologies. Government usage has acted as a driving force for firms and households, with individuals using the Internet to interact with public authorities and many interactions with firms now occurring exclusively online. Nevertheless, important gaps remain, particularly regarding the use of e-commerce by Latvian firms.

However, at present Latvia lacks a national strategy for promoting Internet use among firms and individuals. In addition, the absence of a "whole-of-government" approach means that some opportunities are missed, such as the use of recently digitised cultural heritage resources to connect with the Latvian diaspora. Developing such a strategy will be necessary for Latvia to take full advantage of the digital transformation. A summary of the recommendations from this review is presented in Box 4.10.

Box 4.10. Policy recommendations

Increasing Internet use among individuals

- Use web analytics to evaluate the success of efforts to promote Internet usage.
- Update training resources provided under the Third Father's Son programme and give libraries resources from a national fund to maintain equipment.
- Create a community-based programme targeted especially at older Latvians to boost their use of digital skills, as already exists in Australia and Norway. Give grants to partners (e.g. NGOs or local community groups) and train digital mentors.
- Create a two-pronged digital diaspora programme to link Latvia's inhabitants with family abroad and to disseminate digital cultural resources.
- Link the teaching of digital skills to children with evening training sessions for parents, as has been done in Colombia.

Increasing digital uptake by firms

- Introduce a system whereby business payroll software automatically reports data to Latvia's tax authorities as employees are paid, similar to Australia's Single Touch Payroll system.
- Create a "digital champions" programme, as in Australia, whereby the government supports digital adoption by a small number of SMEs in sectors with low usage of ICTs.

Box 4.10. Policy recommendations *(cont.)*

- Offer consultancy and management advice to laggard firms in sectors with a number of digitally mature firms, to help them catch up with leading firms, as has been done in Australia and Austria.

Reforming the school curriculum

- Pay teachers of STEM subjects an additional allowance to overcome the shortage of such teachers.
- Consult regularly with services and NGOs that directly assist children with digital issues, such as the Safer Internet Centre (Latvijas Drošāka Interneta Centrs), for advice on updating the curriculum.
- Make greater use of career guidance to increase interest among students in ICT-related training and jobs.
- Strengthen links between vocational schools and firms, employing ICT specialists and increasing the proportion of work-based learning.
- Simplify procedures to receive incentives for providing work-based learning.

Reforming higher education

- Support the development of modular degree programmes that include ICTs.
- Give employers a more direct role in influencing university curricula and increase the proportion of time spent by students in work placements.
- Introduce a legal framework for work-based learning in tertiary education.

Improving digital skills among the workforce

- Make greater use of online tools and courses for jobseekers at low risk of long-term unemployment.
- Match data from training and state employment agency databases to improve monitoring of the effects of active labour market policies.
- Create a shared training fund for employees, as in Poland and France, out of employers' contributions to gross wages.
- Abolish labour market tests for foreign ICT workers with adequate experience or qualification, as is the case in Germany and the United Kingdom, and for those that have completed their studies in Latvia.
- Expand tax deductions for higher education tuition fees to include a deduction for student loans.

Improving the delivery of digital government

- Consolidate funding of digital government projects into a single ministry that sets priorities according to a national digital strategy.
- Create a civil service-wide training programme for use of ICTs and the design of services. This can be implemented (as in Colombia) through workshops and virtual courses for public servants, in addition to graduate and postgraduate training.
- Develop a manual of good service delivery practices, as has been done in the United Kingdom, outlining key principles for delivering a good online service and measuring success.
- Create incentives for businesses to interact with government online by prioritising businesses that access services digitally (e.g. by issuing permits or payments more quickly to firms that interact online).
- Develop a timetable for government to deliver services to businesses exclusively online.
- Develop legislation to govern the use of telemedicine, similar to the Act on eHealth and Secure Data Sharing between HealthCare Providers in the Czech Republic.

GOING DIGITAL IN LATVIA © OECD 2021

Box 4.10. Policy recommendations *(cont.)*

- Create a one-stop shop, possibly in association with an HEI, for those who wish to access confidential health and social care data for research, such as is the case in Finland. Support the creation of a social research unit to analyse data generated by digital services and recommend new services.
- Develop pilot programmes for telemedicine.
- Create a prize fund for tertiary-level students who make use of open data in their coursework, as well as for researchers and software developers who use open public data to address societal challenges.
- Host an annual workshop to allow ministries to demonstrate their use of data to improve public services.
- Create an online platform to allow small firms to sell low-value items to central government and municipalities.

References

Andrews, D., G. Nicoletti and C. Timiliotis (2018), "Digital technology diffusion: A matter of capabilities, incentives or both?", *OECD Economics Department Working Papers*, No. 1476, OECD Publishing, Paris, *https://dx.doi.org/10.1787/7c542c16-en*.

Australian Taxation Office (2019), *Single Touch Payroll*, *www.ato.gov.au/Business/Single-Touch-Payroll*.

Bojars, U. and R. Liepins (2014), "The state of open data in Latvia: 2014", *Baltic Journal of Modern Computing*, Vol. 2/3, pp. 160-170.

Burns, T. and F. Gottschalk (eds.) (2019), *Educating 21st Century Children: Emotional Well-Being in the Digital Age*, Educational Research and Innovation, OECD Publishing, Paris, *https://dx.doi.org/10.1787/b7f33425-en*.

Cross-sectoral Coordination Centre (2017), *National Development Plan 2014-2020 Annual and Sustainable Development Strategies for Latvia up to 2030: Annual Implementation Monitoring Report*, Riga.

eParaksts (2020), *Dubultojies pieteikumu skaits eParaksts mobile saņemšanai* [The number of applications for receiving e-Signature mobile has doubled], *eParaksts*, *www.eparaksts.lv/lv/par_mums/Jaunumi/Dubultojies_pieteikumu_skaits_eParaksts_mobile_sanemsanai* (accessed in June 2020).

EsFondi.lv (n.d.), *IKT profesionāļu apmācības inovāciju veicināšanai un nozares attīstībai* [Training of ICT professionals to promote innovation and industry development], *www.esfondi.lv/es-fondu-projektu-mekletajs/project?number=1.2.2.1/16/A/003*.

EsFondi.lv (2015), *Mazo un mikro komersantu apmācības inovāciju un digitālo tehnoloģiju attīstībai Latvijā* [Training of small and micro entrepreneurs for the development of innovations and digital technologies in Latvia], *www.esfondi.lv/es-fondu-projektu-mekletajs/project?number=1.2.2.3/16/I/002*.

EURES (2018), *Short Overview of the Labour Market*, European Employment Services, Brussels, *https://ec.europa.eu/eures/main.jsp?catId=2776&countryId=LV&acro=lmi&lang=en&regionId=LV0&nuts2Code=%20&nuts3Code=&regionName=National%20Level*.

European Commission (2019a), *Digital Economy and Society Index (DESI) Country Report: Latvia*, Brussels.

European Commission (2019b), *eGovernment Benchmark 2019: Empowering Europeans through Trusted Digital Public Services*, Brussels.

European Commission (2019c), *Digital Government Factsheet 2019: Latvia*, Brussels.

European Commission (2018a), *eGovernment in Latvia*, Brussels.

European Commission (2018b), *The Latvian Research Funding System*, Brussels.

European Investment Bank (2019), *The Digitalisation of Small and Medium-sized Enterprises in Portugal: Models for Financing Digital Projects – Summary Report*, Luxembourg, *www.eib.org/attachments/thematic/digitalisation_of_smes_in_portugal_summary_en.pdf*.

Eurostat (2020a), *E-commerce Statistics for Individuals*, Brussels, *https://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals#E-shopping:_biggest_increase_among_young_internet_users* (accessed in June 2020).

Eurostat (2020b), *Hard-to-fill ICT Vacancies: An Increasing Challenge*, Brussels, *https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20200221-1* (accessed in February 2020).

Eurostat (2020c), *ICT Usage in Households and by Individuals* (database), *https://ec.europa.eu/eurostat/cache/metadata/en/isoc_i_esms.htm*.

Eurostat (2019a), *Individuals' Level of Digital Skills* (database), *https://data.europa.eu/euodp/en/data/dataset/O6Pzf6zY9zRfr8Wg9X5gw*.

Eurostat (2019b), *ICT Specialists in Employment*, Brussels, *https://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_specialists_in_employment* (accessed in October 2019).

Eurostat (2019c), *E-Commerce Statistics* (database), *https://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics*.

Finance Latvia Association (2019), *Finance Latvia Supports the New Program of Excellence*, *www.financelatvia.eu/en/news/finance-latvia-supports-the-new-program-of-excellence* (accessed in August 2019).

gov.uk (2020), *Immigration Rules Appendix K: Shortage Occupation List*, *www.gov.uk/guidance/immigration-rules/immigration-rules-appendix-k-shortage-occupation-list* (accessed in March 2020).

Government Digital Service (2019), "Design and build government services", *www.gov.uk/service-toolkit* (accessed in March 2020).

Jacobs, B. et al. (2017), *Latvia Tax Review*, World Bank Group, *http://documents1.worldbank.org/curated/en/587291508511990249/pdf/120580-WP-P158470-PUBLIC-117p-WBLatviareportPOP.pdf*.

Kässi, O. and V. Lehdonvirta (2018), *Online Labour Index: Measuring the Online Gig Economy for Policy and Research*, *https://mpra.ub.uni-muenchen.de/86627* (accessed on 20 June 2018).

KISC (2019a), *Bibliotekāriem piedāvā IT drošības apmācības e-vidē* [Librarians are offered IT security training in the e-environment], Kultūras informācijas sistēmu centrs, *www.kis.gov.lv/2019/03/bibliotekariem-piedava-it-drosibas-apmacibas-e-vide* (accessed in August 2019).

KISC (2019b), *Kultūras informācijas sistēmu centrs* [Centre for Cultural Information Systems], *www.kis.gov.lv*.

KISC (2015), *Publisko bibliotēku attīstības projekts "Trešais Tēva Dēls"* [Public library development project "Third Father's Son"], Kultūras informācijas sistēmu centrs.

LCCI (2019), *LTRK turpina īstenot nodarbināto apmācību projektu* LCCI continues to implement the employee training project], Latvian Chamber of Commerce and Industry, Riga, *www.chamber.lv/lv/content/3403*.

LCCI (2017), *Productivity Evolution 2*, Latvian Chamber of Commerce and Industry, Riga, *www.chamber.lv/en/content/851* (accessed in October 2019).

LIKTA (2019), *Project Women4IT*, Latvian Information and Communication Technology Association, Riga, *https://likta.lv/en/project-women4it* (accessed in October 2019).

LIKTA (2018), *Young ICT Women*, Latvian Information and Communication Technology Association, Riga, *https://likta.lv/en/young-ict-women* (accessed in October 2019).

Menshikov, V. and O. Volkova (2019), "Digitalization for increased access security to healthcare services in Latvia", *Journal of Security & Sustainability Issues*, Vol. 9/1, pp. 171-183.

MoE (2018), *Informative Report On Medium And Long-Term Labour Market Forecasts*, Ministry of Economy, Riga, *www.em.gov.lv/en/economic_development/labor_market/informative_report_on_medium_and_long_term_labour_market_forecasts*.

MoES (2020), *Description of Educational Curriculum and Learning Approach*, Ministry of Education and Science, Riga, *www.izm.gov.lv/en/highlights/3336-description-of-educational-curriculum-and-learning-approach-2* (accessed on 11 May 2020).

MoF (2018), *Tax System in Latvia*, Ministry of Finance, Riga, *www.fm.gov.lv/en/s/taxes* (accessed in October 2019).

NIFO (2018), *Latvian Automated Translation Service*, National Interoperability Framework Observatory, *https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/document/latvian-automated-translation-service*.

OECD (2020), *OECD Structural and Demographic Business Statistics (SDBS)* (database), OECD, Paris, *https://stats.oecd.org/Index.aspx?DataSetCode=SSIS_BSC_ISIC4* (accessed on 6 May 2020).

OECD (2019a), *OECD Skills Outlook 2019: Thriving in a Digital World*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/df80bc12-en*.

OECD (2019b), *OECD Reviews of Digital Transformation: Going Digital in Colombia*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/781185b1-en*.

OECD (2019c), *OECD Economic Surveys: Latvia 2019*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/f8c2f493-en*.

OECD (2019d), *OECD SME and Entrepreneurship Outlook 2019*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/34907e9c-en*.

OECD (2019e), *Innovation, Agricultural Productivity and Sustainability in Latvia*, OECD Food and Agricultural Reviews, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264312524-en*.

OECD (2019f), *OECD Digital for SMEs Global Initiative*, OECD Publishing, Paris, *www.oecd.org/going-digital/sme/resources/D4SME-Brochure.pdf*.

OECD (2019g), *Education at a Glance 2019: OECD Indicators*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/f8d7880d-en*.

OECD (2019h), *PISA 2018 Results (Volume I): What Students Know and Can Do*, PISA, OECD Publishing, Paris, *https://dx.doi.org/10.1787/5f07c754-en*.

OECD (2019i), *OECD Skills Strategy Latvia: Assessment and Recommendations*, OECD Skills Studies, OECD Publishing, Paris, *https://doi.org/10.1787/74fe3bf8-en*.

OECD (2019j), *TALIS 2018 Results (Volume I): Teachers and School Leaders as Lifelong Learners*, TALIS, OECD Publishing, Paris, *https://dx.doi.org/10.1787/1d0bc92a-en*.

OECD (2019k), *Evaluating Latvia's Active Labour Market Policies*, Connecting People with Jobs, OECD Publishing, Paris, *https://dx.doi.org/10.1787/6037200a-en*.

OECD (2019l), *Education Policy Outlook 2019: Working Together to Help Students Achieve their Potential*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/2b8ad56e-en*.

OECD (2019m), *Getting Skills Right: Future-Ready Adult Learning Systems*, Getting Skills Right, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264311756-en*.

OECD (2019n), *OECD Skills Strategy Latvia: Assessment and Recommendations*, OECD Skills Studies, OECD Publishing, Paris, *https://dx.doi.org/10.1787/74fe3bf8-en*.

OECD (2019o), *Government at a Glance 2019*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/8ccf5c38-en*.

OECD (2019p), *Health in the 21st Century: Putting Data to Work for Stronger Health Systems*, OECD Health Policy Studies, OECD Publishing, Paris, *https://dx.doi.org/10.1787/e3b23f8e-en*.

OECD (2019q), *Going Digital Toolkit* (database), OECD, Paris, *https://goingdigital.oecd.org/en*.

OECD (2019r), *The Path to Becoming a Data-Driven Public Sector*, OECD Digital Government Studies, OECD Publishing, Paris, *https://dx.doi.org/10.1787/059814a7-en*.

OECD (2018a), *ICT Access and Usage by Households and Individuals* (database), OECD, Paris, *http://oe.cd/hhind*.

OECD (2018b), "Digitalisation", *Latvia Policy Brief*, OECD, Paris, *www.oecd.org/policy-briefs/Latvia-digitalisation.pdf*.

OECD (2018c), *Skills for Jobs – Latvia Country Note*, OECD, Paris, *www.oecdskillsforjobsdatabase.org/data/country_notes/Latvia%20country%20note.pdf*.

OECD (2018d), "Latvia", in *Education at a Glance 2018: OECD Indicators*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/eag-2018-56-en*.

OECD (2018e), *Skills for Jobs Database*, OECD, Paris, *www.oecdskillsforjobsdatabase.org* (accessed in March 2020).

OECD (2018f), *Seven Questions about Apprenticeships: Answers from International Experience*, OECD Reviews of Vocational Education and Training, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264306486-en*.

OECD (2018g), *SMEs in Public Procurement: Practices and Strategies for Shared Benefits*, OECD Public Governance Reviews, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264307476-en*.

OECD (2017a), *OECD Economic Surveys: Latvia 2017*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/eco_surveys-lva-2017-en*.

OECD (2017b), *OECD Economic Surveys: Slovenia 2017*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/eco_surveys-svn-2017-en*.

OECD (2017c), *ICT Access and Use by Businesses* (database), OECD, Paris, *http://oe.cd/bus*.

OECD (2016a), "New Skills for the Digital Economy: Measuring the demand and supply of ICT skills at work", *OECD Digital Economy Papers*, No. 258, OECD Publishing, Paris, *https://dx.doi.org/10.1787/5jlwnkm2fc9x-en*.

OECD (2016b), *OECD Reviews of Labour Market and Social Policies: Latvia 2016*, OECD Reviews of Labour Market and Social Policies, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264250505-en*.

OECD (2016c), *Recommendation of the Council on Health Data Governance*, OECD, Paris, *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0433*.

Office of Citizenship and Migration Affairs (2020), *No 2023.gada 1.janvāra personas apliecība (eID karte) būs obligāts personu apliecinošs dokuments* [From January 1, 2023, the identity card (eID card) will be a mandatory identity document], Riga, *www.pmlp.gov.lv/lv/sakums/jaunumi/aktualitates/2020/02/26/no-2023.gada-1.janv%C4%81ra-personas-apliec%C4%ABba-(eid-karte)-b%C5%ABs-oblig%C4%81ts-personu-apliecino%C5%A1s-dokuments* (accessed in June 2020).

Oliveira Hashiguchi, T. (2020), "Bringing health care to the patient: An overview of the use of telemedicine in OECD countries", *OECD Health Working Papers*, No. 116, OECD Publishing, Paris, *https://dx.doi.org/10.1787/8e56ede7-en*.

Perry, G. (ed.) (2017), *Informality, Productivity, and the Firm*, The World Bank, Washington, DC.

Randall, L. and A. Berlina, (2019), *Governing the Digital Transition In Nordic Regions: The Human Element*, Nordregio, Stockholm, *http://norden.diva-portal.org/smash/get/diva2:1295022/FULLTEXT01.pdf*.

Sauka, A. and T. Putniņš (2019), *Shadow Economy Index for the Baltic Countries 2009–2018*, Stockholm School of Economics, *www.sseriga.edu/shadow-economy-index-baltic-countries*.

State Chancellery (2017), *The Government Approves Latvia's Third National Action Plan for Open Government Partnership*, Riga, *www.mk.gov.lv/en/aktualitates/government-approves-latvias-third-national-action-plan-open-government-partnership*.

Valdani Vicari and Associati (2019), *Monitoring Progress in National Initiatives on Digitising Industry: Country Report Latvia*, *https://ec.europa.eu/information_society/newsroom/image/document/2019-32/country_report_-_latvia_-_final_2019_0D30BE44-054B-C822-C8DEFA25536D65B0_61211.pdf*.

VARAM (2013), *Information Society Development Guidelines 2014-2020 (Informative part)*, Ministry of Environmental Protection and Regional Development, Riga, *www.varam.gov.lv/in_site/tools/download.php?file=files/text/Darb_jomas/elietas//Information_Society_Development_Guidelines_2014_2020.docx*.

VISC (2019), *Par projektu* [About the project], State Education Content Center, Riga, *www.skola2030.lv/lv/par-projektu* (accessed on 11 May 2020).

VRAA (2019), *e-Zinas*, State Regional Development Agency, Riga, *www.vraa.gov.lv/uploads/documents/latvijalv10/vraa_e-zinas_2019_4_cet.pdf*.

World Economic Forum (2017), *The Global Competitiveness Index Historical Dataset 2007-2017*, *https://tcdata360.worldbank.org/indicators/fin.loc.eqy.mkt?country=BRA&indicator=525&viz=line_chart&years=2007,2017*.

WKO (2018), "Aktuelles zur neuen Ausbildung im Lehrberuf E-Commerce-Kaufmann/-frau" [Current information on the new apprenticeship as an e-commerce businessman/woman], *Wirtschaftskammer Österreich*, *www.wko.at/branchen/handel/lehrberuf-e-commerce-kaufmann-frau.html* (accessed in March 2020).

Zech, T. (2020), "Skilled personnel welcome", deutschland.de, *www.deutschland.de/en/topic/business/the-skilled-labour-immigration-act-working-in-germany* (accessed in March 2020).

Note

Israel
The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

Chapter 5

ENHANCING TRUST IN THE DIGITAL ECONOMY

Latvia's digital security policies

This section provides an overarching description and analysis of digital security policy in Latvia. The first *Cyber Security Strategy of Latvia*, covering the period 2014-18, took stock of the digital transformation, and marked a shift towards a more strategic and whole-of-government approach to digital security. The second *Cyber Security Strategy of Latvia*, covering 2019-22, continues this trajectory, with a greater emphasis on risk management, resilience, public awareness, and the need to balance digital security with openness, prosperity and human rights.

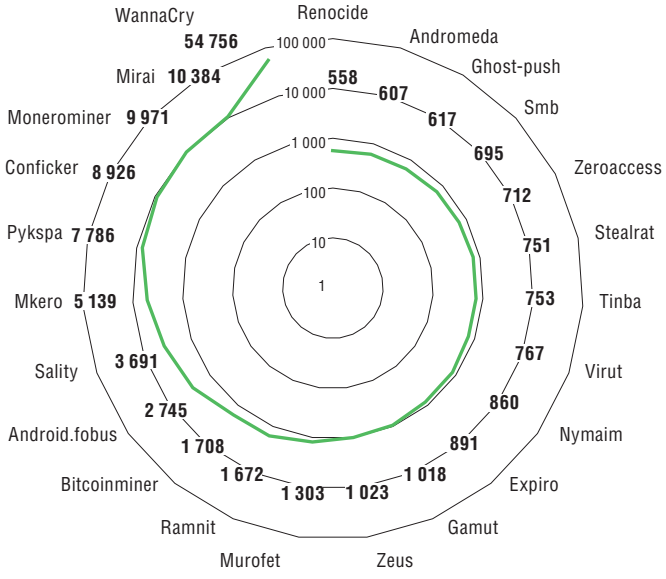
These strategies are representative of the advancement in the Latvian government's approach to digital security policy. However, the economic and social risks of digital security are not yet fully integrated into these documents or their processes for implementation. In fact, Latvia's geopolitical environment has led the government to rely mainly on a national security conceptual framework that focuses on critical infrastructures and state institutions. Multi-stakeholder engagement and market-oriented policies could be strengthened in order to fully realise the potential of the digital transformation. This would also help increase the ownership of digital security risk by senior leadership in organisations and businesses, especially SMEs.

Recent trends

Digital security attacks in Latvia

In 2018-19, media attention in Latvia focused on attacks by politically motivated entities from countries "having an opposite political ideology to that of NATO and the EU" (CERT.LV, 2018). Examples include operations targeting the electoral process in the Saeima, Latvia's Parliament. However, a thorough analysis suggests that, like many other countries, Latvia suffered from attacks which had a more global reach, such as WannaCry and Mirai[1] (Figure 5.1). However, the number of organisations affected by such attacks in Latvia was relatively low. The main victims of digital security incidents in Latvia were small and medium enterprises (SMEs) and municipalities (CERT.LV, 2018).

Figure 5.1. Most common malicious code attacks in Latvia, 2018

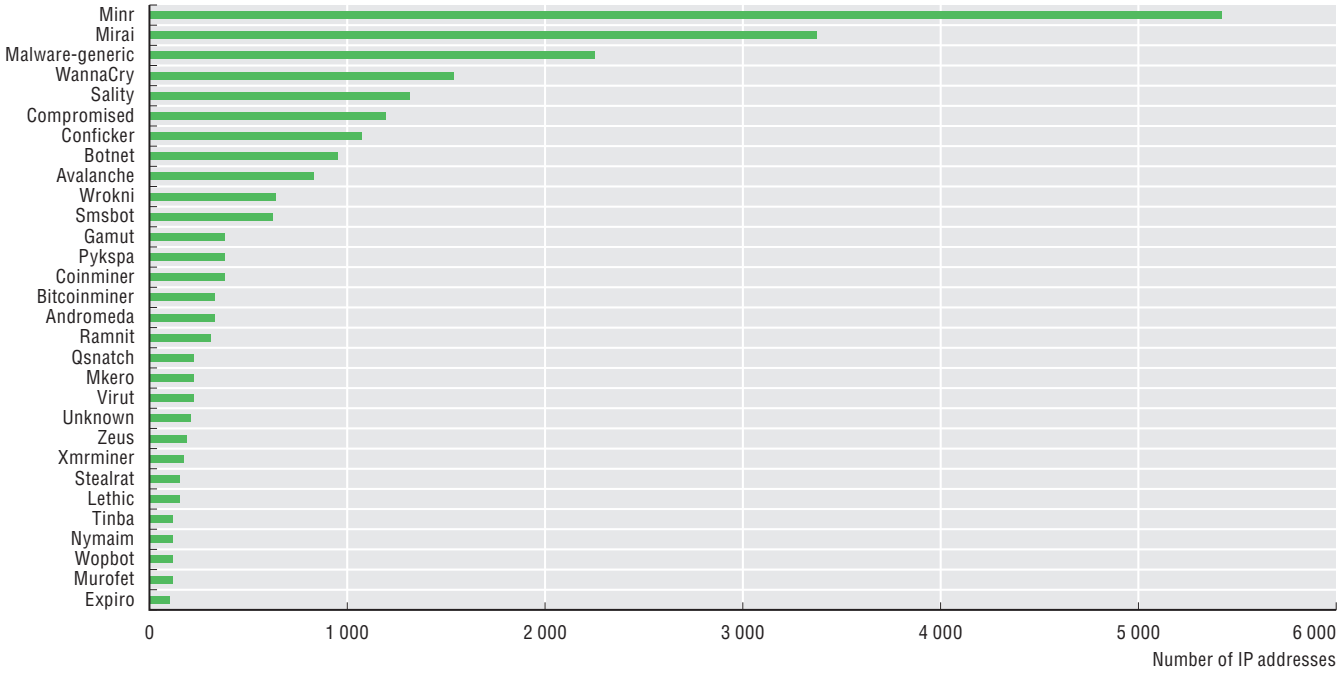


Source: CERT.LV (2018), *CERT.LV Public Performance Report*, *https://cert.lv/uploads/cert-gada-parskats-2019.pdf*.

More recent data (Figure 5.2) confirm that the main forms of malware targeting Latvian organisations match those in other countries, with Mirai and WannaCry being, respectively, the second and fourth most common malwares in the first quarter of 2020. The dominant position of Minr as the most common malicious code in Latvia during this period illustrates the global trend of cryptocurrency mining malware.

Figure 5.2. Most common malicious code attacks in Latvia, Q1 2020

Number of unique IP addresses threatened by malicious code



Source: CERT.LV (2020), *CERT.LV reģistrētie incidenti no 01.01.2020. līdz 31.03.2020*, *https://cert.lv/lv/2020/04/pieejama-statistika-par-2020-gada-1-ceturksni*.

Key dates for digital security policy in Latvi

Digital security is a not a new policy area in Latvia. Prior to 2012, the Latvian approach to digital security focused mainly on technical aspects and infrastructure. The Ministry of Transport (MoT) was the institution responsible for overall co-ordination of digital security policy.

In 2010, Latvia adopted the Law on the Security of Information Technology ("IT security law"), which entered into force in 2011 and serves as the main legal framework for digital security (see the section on the legal framework). It resulted, *inter alia*, in the establishment of:

- the Latvian Computer Emergency Response Team, CERT.LV,[2] which is hosted by the Institute of Mathematics and Computer Science of the University of Latvia and was placed under the authority of the Ministry of Defence
- the National Information Technology Security Council (NITSC), a body which meets at least once every four months and is mainly composed of high-level representatives of ministries and other public organisations involved in digital security policy.

In 2013, the Latvian Cabinet of Ministers approved the *Information Society Development Guidelines 2014-2020* (VARAM, 2014), which serve as a national digital strategy. The adoption of the guidelines represented in shift in perspective with the recognition that digitalisation affects all parts of society. Digital security risks became a strategic public policy issue requiring the involvement of many ministries through a whole-of-government approach.

This shift was confirmed in 2014 with the adoption of the *Cyber Security Strategy of Latvia (2014-2018)*, which states that "the idea that ICT is a matter of interest of just a small groups of professionals has been gradually substituted by the understanding that the entire society is, to a greater or lesser extent, linked with ICT" (MoD, 2014). Logically, the first objective of the strategy was to build a clear governance framework for digital security in Latvia. This new governance framework was structured around the NITSC, under the overarching supervision of the Ministry of Defence (MoD), which took over the co-ordinating role in the definition and implementation of the digital security policy in Latvia.

In 2016, the MoD, in co-operation with other ministries and the NITSC, undertook a mid-term review of the implementation of the strategy; then, in 2019, the Latvian Cabinet of Ministers approved a report on the strategy's implementation which considered that most of the objectives had been met or are in the process of being executed. However, the report also recognised obstacles to meeting certain objectives, in particular: 1) that digital security is not always a priority for decision makers; 2) a lack of digital security skills; and 3) a lack of funding for digital security.

Building on these elements, in 2019 the Latvian Cabinet of Ministers the second *Cyber Security Strategy of Latvia (2019-2022)*. Prepared by the MoD in co-operation with other ministries and the NITSC, this document sets out the national priorities for digital security policy in Latvia and identifies upcoming challenges. The new strategy's main objective is to strengthen and improve digital security capabilities by boosting resilience against attacks and enhancing public awareness of threats in cyberspace.

This reflects a positive evolution in Latvia's approach to digital security. The development of the two cyber security strategies and the leadership role played by the MoD since 2013 has made digital security a strategic priority in Latvia. However, national security has been foregrounded at the expense of other aspects, notably economic and social prosperity (Figure 5.3). This is confirmed by an analysis of the set of definitions related to digital security provided in Latvian policy documents (see next subsection).

Digital security and associated terms in Latvia's policies

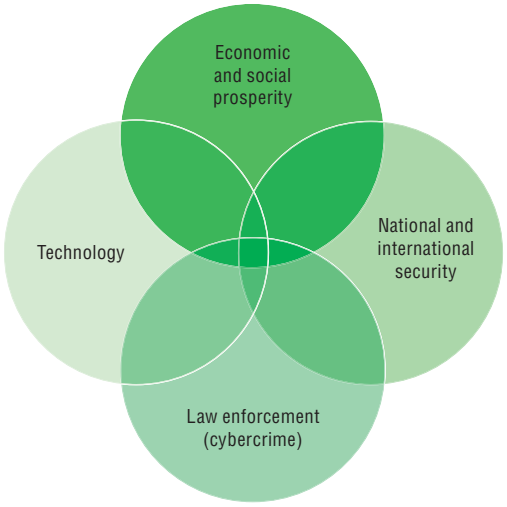
Latvian policy documents rely on the concepts of "cyber security", "security of information technologies" and "information security" (MoD, 2014; VARAM, 2014).

In its 2015 *Recommendation on Digital Security Risk Management for Economic and Social Prosperity*, thereafter "the 2015 Recommendation" (OECD, 2015), the OECD uses the term "digital security" rather than "cyber security", "information security" or "IT security". The OECD defines "digital security" as the management of economic and social risks resulting from breaches of availability, integrity and confidentiality (AIC) of information and communication technologies (ICTs) and data. This definition represented a shift from the 2002 OECD *Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security* ("Security Guidelines") (OECD, 2002), which focused mostly on technical aspects rather than managing digital security risks to economic and social activities reliant on the use of ICTs.

However, there is no universally agreed terminology to capture the different facets of digital security in every context. Terms vary across countries, and reflect different government cultures and histories: there is no "right" or "wrong" terminology. In 2015, OECD countries favoured "digital" over "cyber" as the latter is often associated with concepts such as "cyber warfare", "cyber defence" or "cyber influence". Furthermore, "cyber" is absent from economic circles, which more generally stick to the digital semantic: digital economy, digital transformation, digitalisation and so on. "Digital" facilitates the recognition of "digital security" as an economic issue by policy makers and business leaders. "Information security" was left aside as a technical management term primarily reflecting the view of the technical community (e.g. ISO/IEC 27000 Information Security Management Systems standards). "Information security" also carries ambiguity in an international context as it has a different scope in countries such as the People's Republic of China and the Russian Federation, which use it also to capture policies against disinformation, influence and information manipulation. Disinformation, influence and the spread of harmful content are important issues exacerbated by the digital transformation. They can sometimes overlap with digital security, for example, when digital security attacks are used to alter the integrity of data in order to manipulate public opinion or to prevent access to government services. They are, however, different from the management of the economic and social consequences of breaches of AIC, as they involve different policy tools and legal considerations related to free speech and media regulation.

Beyond semantics, the communities addressing each dimension of digital security (Figure 5.3) often have different cultures and backgrounds, and their objectives can sometimes converge, overlap or compete, depending on the context and precise issue. Cryptography policy (OECD, 1998) is a typical example of competing objectives, with businesses, organisations and consumers promoting the unregulated use of cryptography to support trust and facilitate e-commerce, digital governments and innovation online, while law enforcement and intelligence agencies advocate regulation to facilitate access to encrypted data in order to combat criminals and terrorism.

Figure 5.3. The four dimensions of "cybersecurity"



In Latvian policy documents, the concepts of "cyber security", "IT security" and "information security" seem to refer, depending on the context, to either one of these definitions:

- the protection of technical assets, such as networks, ICTs and data (the "Technology" facet of Figure 5.3)
- the management of risks related to the use of ICTs, which do not focus on economic and social activities, but instead touch upon issues relating to national security, influence over strategies in democratic elections and harmful content (the "National security" and "Law enforcement" facets of Figure 5.3).

For instance, the *Cyber Security Strategy of Latvia (2014-2018)* defined cyber security as "the collection of tools, policies, concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and users' assets". Alternatively, the *Cyber Security Strategy of Latvia (2019-2022)* relies on a "vision of cyber security policy as a secure, open, free and reliable cyberspace that guarantees the safe, reliable and continuous receipt and delivery of services essential to the state and society, and respects the individual's human rights in a physical and virtual environment". The latter document also acknowledges that "Latvia needs to take advantage of the digital environment to ensure economic and social welfare, while at the same time reducing the overall level of cybersecurity risk without unnecessarily limiting the flow of technology, communications and data".

This shift is a positive development, with the Latvian government now recognising that digital security impacts other aspects of the digital economy (openness, freedom), suggesting that a risk-based approach is warranted and that trade-offs are necessary. The strategy also acknowledges the emergence of cyber-physical systems, which make the virtual (or "cyberspace")/physical dichotomy less relevant, as more and more economic and social activities "go digital". Overall, this semantic evolution reflects a deeper change in the way that Latvia approaches digital security, recognising it as an enabler of the digital transformation, rather than as an end in itself.

Governance

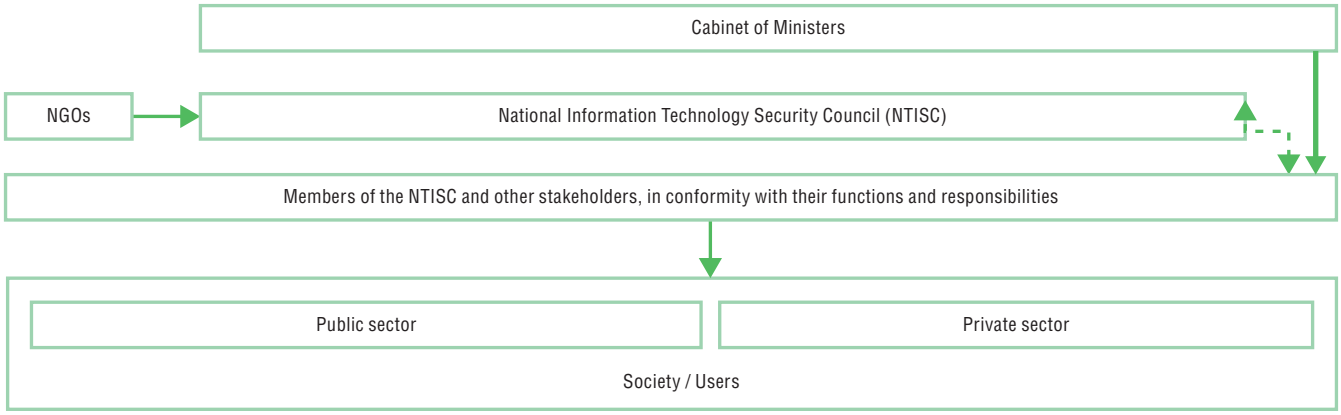
Overall governance framework for digital security policy in Latvia

Since 2014, the MoD has co-ordinated the development and implementation of digital security policy, involving many ministries across the Latvian government.[3]

In order to co-ordinate the development of policies related to digital security in Latvia, and manage potential conflicts between institutions, the NITSC was established. This council has been described alternatively as a permanent high-level working group and a formal body. The NITSC is chaired by the MoD, usually at the level of the Secretary of State. It meets at least once every four months and gathers together – usually high-level – representatives from numerous institutions, including ministries and

law enforcement agencies. Other stakeholders are invited to participate on an ad-hoc basis,[4] as the main function of the NITSC is to ensure effective intragovernmental co-operation. Figure 5.4 provides a visual representation of the governance framework for digital security in Latvia (MoD, 2019).

Figure 5.4. Digital security governance framework for Latvia (2019-2022)



Note: NGO = non-governmental organisation.

Source: MoD (2019), *Cyber Security Strategy of Latvia (2019-2022)*, *https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf*.

The NITSC has no specific dedicated budget, and administrative support is provided by the MoD. The National Cyber Security Policy Co-ordination (CSPC) section within the MoD provides support on behalf of the secretariat for the NITSC. The MoD also ensures the work of the Supervisory Committee of Electronic Identification.

The Ministry of Foreign Affairs (MFA) co-ordinates digital security-related international co-operation, with the involvement of the MoD for NATO and EU-related digital security issues.

The Ministry of Environmental Protection and Regional Development (VARAM) is responsible for state information systems and co-ordinates the digitisation of public services. The State Regional Development Agency (SRDA) ensures the operation and development of solutions for shared use of state ICT, including the national eID and digital signature platform, the national eIDAS gateway, the public procurement system and the public services portal Latvija.lv as well as the official eAddress solution. The VARAM also leads the overall development of a digital and information society policy, and the Deputy State Secretary of VARAM is the deputy chair of the NITSC.

The Ministry of the Interior (MoI) and the State Police (SP) implement law enforcement policies to tackle cybercrime.

CERT.LV provides support to state authorities in the detection of digital security incidents. CERT.LV is also responsible for organising responses in the event of digital security incidents, including crisis management. It monitors and analyses developments in digital security, produces statistics on and reacts to incidents and co-ordinates their prevention, carries out research, organises educational events and training, and supervises the implementation of obligations specified under the Law on the Security of Information Technology. Beyond its primary mission to provide support for public institutions, CERT.LV also supports entrepreneurs and individuals. The budget of CERT.LV has increased significantly over recent years, from approximately EUR 120 000 in 2011 to EUR 882 000 in 2015 and 1 328 000 in 2019, reflecting the commitment of the Latvian government to increasing digital security capabilities.

The Constitution Protection Bureau (CPB), the national intelligence and security agency, oversees the protection of critical infrastructures. The CPB also actively participates in co-operation initiatives between the Baltic States and the United States, by providing expertise and guidance in the field of critical energy infrastructure. CPB and CERT.LV work together to test the resilience of critical information technology infrastructures and provide guidance to public and private operators of such infrastructures.

The Ministry of Welfare (MoW) implements social policy and policy for the protection of children online.

The Latvian State Radio and Television Centre (LSRTC), a state joint-stock company, is the only provider of qualified trust services (i.e. electronic signatures, seals and forms of identification).

The National Armed Forces (NAF) and the National Guard Cyber Defence Unit (CDU) provide support in the event of crises. While the main responsibility of NAF is to develop and strengthen military information technology and communication systems and networks, NAF also plays a significant role in enhancing overall cyber defence capabilities.

Towards a whole-of-government and multi-stakeholder approach

In order for digital security strategies to be successful, it is necessary to engage effectively with all relevant actors across government *and* within the broader multi-stakeholder community (i.e. instance researchers, businesses, civil society, etc.). While many strategies recognise the importance of this two-pronged approach (whole-of-government co-ordination and multi-stakeholder engagement), effective implementation can prove challenging, as it requires adequate resources, trust and, sometimes, a cultural shift.

The current governance framework for digital security policy in Latvia, described in the previous section, partially fits the whole-of-government approach, and could be described as "partially centralised" (MoD, 2014). The creation and implementation of this framework in 2012-14 marked a turning point in Latvia's approach: digital security was no longer considered solely a technical problem of institutions in charge of networks (the Ministry of Transport); instead, it became a public policy issue requiring the involvement of the entire government.

Within this framework, the Latvian approach, so far, has consisted of emphasising national security aspects, which has helped digital security risk gain momentum as a key policy issue, and leveraging resources within government. As an illustration, the NITSC is chaired by the Secretary of State of the MoD, which in turn supervises CERT.LV.

While this approach has brought undeniable benefits, it also has some shortcomings. Approaching digital security mainly through a national security framework may limit the ability of stakeholders to fully engage and own digital security risk, as national security is often associated with state matters. For instance, industry and civil society stakeholders are usually only invited on an ad-hoc basis to NITSC meetings, and do not participate in the design and implementation of the strategy. While stakeholders are invited to participate in this process through public comments, effective participation is often low. Such limited engagement could result from a lack of long-term, trust-based and sustainable multi-stakeholder partnerships, which are fundamental to enabling meaningful and effective participation (OECD, 2015). It could also result from an insufficiently co-ordinated and structured multi-stakeholder community. The national security focus may also limit the ability of other parts of the government to approach digital security as an economic opportunity (e.g. research, innovation, skills entrepreneurship, etc.). If there is insufficient co-operation with and involvement on the part of ministries in charge of economic development and sectoral co-ordination, there is also a risk that these ministries will not develop the requisite technical skills and understanding of the challenges involved, to participate meaningfully in the design and implementation of the digital security strategy.

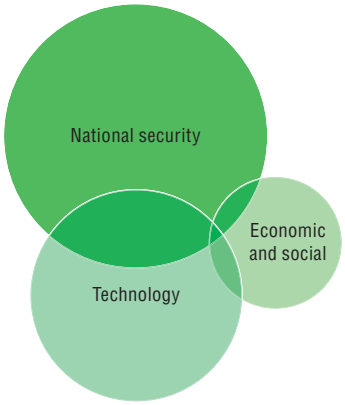
To summarise, the current approach in Latvia (Figure 5.5) is structured around a national security framework (NITSC) which relies on a strong technical foundation (CERT.LV). However, the economic and social dimension seems less present, and the policy is usually implemented through a technical (via CERT.LV) or national security lens.

Most governments have struggled to establish an appropriate governance framework for digital security, as it is difficult to strike the right balance between economic and social concerns, national security, law enforcement and technical facets (Figure 5.3). There is no one-size-fits-all model, and governance frameworks and co-ordination mechanisms vary considerably across OECD countries, reflecting national history, geopolitical context, style of government and maturity in this area.

In many OECD countries, the process of building a digital security governance framework often starts with the national security, cybercrime (e.g. adoption of a cybercrime legislation) or technological dimension, focusing on increasing technical response capacity, for example through creating a computer emergency response team (CERT). The process then expands gradually to encompass economic and

social prosperity. However, some countries reached a consensus that national security-oriented agencies were not necessarily best placed to develop and implement economic and social policies, arguing that this was not their core mission and that they too often lacked the culture of transparency and multi-stakeholder engagement essential to building trust-based and sustainable partnerships.

Figure 5.5. Digital security policy in Latvia



Notes: This figure illustrates the degree of government attention to three of the four components of the digital security framework, as shown in Figure 5.3. Criminal law enforcement, which is included in Latvia's current framework, is not shown as it is beyond the scope of this review.

In order to address all facets of cyber security holistically, rather than in a fragmented manner, digital security strategies must be supported at the highest level of government (i.e. the head of state or head of government), and establish new governance and co-ordination mechanisms to ensure balance between complementary and sometimes competing objectives across the different dimensions (OECD, 2015; 2012) However, each country must adopt a governance model tailored to its culture and style of government.

For example, Australia, Japan and the United Kingdom assigned policy co-ordination to the Prime Minister through the Cabinet Office. France established a national co-ordination agency within a pre-existing co-ordination body under the Prime Minister (ANSSI). The United States set up a "Cybersecurity and Infrastructure Security Agency" (CISA) within the Department of Homeland Security. Canada, Germany and the Netherlands placed the main responsibility for digital security under an existing ministry (respectively, the ministries of Public Safety, the Interior, and Security and Justice). Israel created a national agency reporting directly to the Prime Minister (INCD).

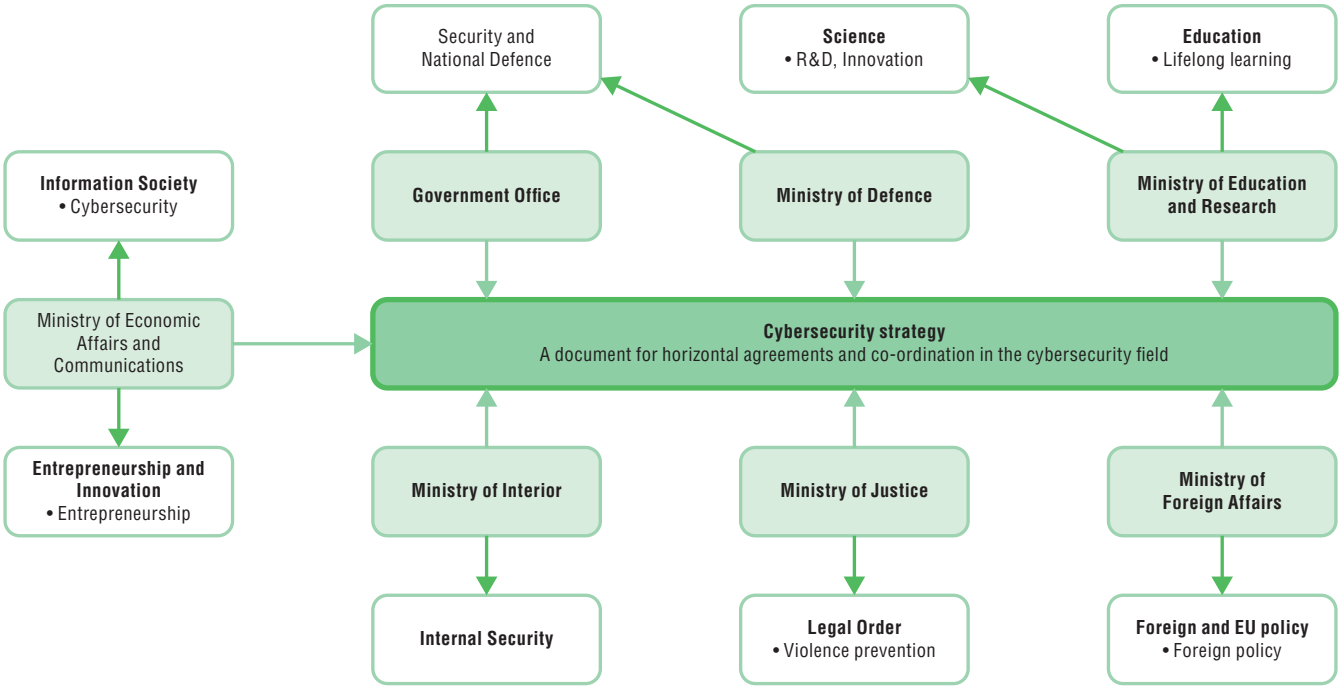
In Denmark, responsibility for overall co-ordination of the digital security strategy is split between the Agency for Digitisation (within the MoF) and the Centre for Cyber Security (MoD). The agency is in charge of digital security in the public sector and is responsible for a number of citizen-focused initiatives. The centre advises public authorities and private companies that support critical activities. The agency chaired the working group that developed the digital security strategy.

In Estonia, the Ministry of Economic Affairs is in charge of co-ordinating the development and implementation of digital security policy (Figure 5.6). The other ministries (Defence, Research, Education, Interior, Justice, etc.) are also fully involved within their own domain of competence.

In all these cases, there are also different arrangements with respect to how multi-stakeholder co-ordination is concretely carried out, and where government operational capacity is located. This ranges from within the policy co-ordination agency (France, Israel) to a sub-structure attached or reporting to the ministry (Germany, the Netherlands), or a separate structure (the UK National Cyber Security Centre). Furthermore, policies to foster the digital security of critical activities and infrastructure create a need to engage sectoral regulators (e.g. in the telecommunications, health, finance, transport and energy sectors) to ensure that related digital security regulation takes into account existing market and regulatory constraints.

Economic-oriented and multi-stakeholder-driven initiatives have been launched in many OECD countries. Governments have facilitated sector-specific partnerships aimed at sharing information and best practices for digital security challenges, for example through Information Sharing and Analysis Centres (ISAC). Another good practice is to launch partnerships with Internet service providers (ISPs) and other stakeholders to detect and clean infected connected devices. For instance, the Dutch Government has taken steps to monitor and enhance the digital security of connected devices through a public-private partnership that includes ISPs, the Ministry of Economic Affairs and the University of Delft. The goal of this initiative is to share information across manufacturers/vendors as well as with end users, to encourage product distributors to consider removing affected products from the shelves, and incentivise consumers to patch or deactivate products if critical vulnerabilities are discovered.

Figure 5.6. Governance framework for digital security policy in Estonia



Source: MoEAC (2019), *Cyber Security Strategy of Estonia (2019-2022)*, *www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf*.

In Latvia, the current governance framework is indicative of a willingness to engage with the multi-stakeholder community, although the means to ensure their effective participation could be enhanced. While the NITSC is described in the *Cyber Security Strategy* as "the central national authority for the exchange of information and co-operation between the public and private sector", it seems that non-governmental stakeholder groups (the private sector as well as civil society) are only invited to participate on an ad-hoc basis. They do not fully contribute to the design and implementation of the strategy, even though they are invited to do so through public comments. This could indicate that the multi-stakeholder community is not structured enough to sufficiently participate in digital security policy making. In addition, the NITSC only meets once every four months, and serves mostly as a channel to discuss issues within government, rather than as an agile and business-friendly or civil society-friendly forum. This may also explain in part why business leaders in Latvia do not necessarily consider digital security as their own priority, as it is presented in the governance framework mainly as a national security issue.

Finally, various policy documents describe the NITSC alternatively as a "consultative" body, a "co-ordination" platform, the authority monitoring the "implementation" of the Cyber Security Strategy and the body in charge of evaluating digital security policy implementation. The governance framework does not clearly separate the functions of design, consultation, implementation and evaluation of the digital security strategy, as the NITSC, under the leadership of the MoD, seems to perform all these

functions. This may lead to limited external oversight and a lack of valuable feedback, and hence hinder improvement of the strategy over time.

Legal framework

The main legal framework for digital security in Latvia is the Law on the Security of Information Technologies, adopted in 2010 and amended several times since. The law applies to national and local government authorities, operators of critical infrastructure of information technologies (CIITs), operators of essential services and digital service providers, as well as electronic communications providers. It designates key organisations and their responsibilities in the area of digital security (e.g. NITSC and CERT.LV).

The Law on State Information Systems, adopted in 2002 and amended in 2014, relates to the networks used and maintained by governmental authorities. Among other provisions, it determines the unified procedures by which national information systems are created, registered, maintained, used, reorganised or discarded, and governs their management of digital security.

Other relevant regulations of note include:

- Cabinet regulation No. 422: "Procedures to ensure minimal security requirements of information and communication technologies' systems" (2015, updated in 2017 and 2019), which has the goal of harmonised and higher security levels in ICT systems across state and municipal institutions
- Cabinet Regulation No. 764: "General Technical Requirements of State Information Systems" (2005, latest amendments in 2009)
- Cabinet Regulation No. 496: "Procedures for the Identification of Critical Infrastructures, Including European Critical Infrastructures and Planning and Implementation of Security Measures" (2010, amended since)
- Cabinet Regulation No. 100: "Procedures for the planning and implementation of security measures of the information technologies of critical infrastructure" (2011).

A thorough audit of existing laws and regulations in the field of digital security, and their implementation, has apparently not yet been undertaken by the Latvian authorities.

Recent initiatives

Information Society Development Guidelines (2014-2020)

The *Information Society Development Guidelines* (2014-2020) serve as the Latvian national digital strategy. Their main objective is "to provide an opportunity for everyone to use the possibilities offered by ICTs, to develop a knowledge-based economy and to improve the overall quality of life by contributing to the national competitiveness, and increasing an economic growth and job creation". However, the Guidelines focus mainly on enhancing access and use of ICTs as well as e-government services such as online identity and state ICTs.

Action Direction 5.7 of the Guidelines relates to "Trust and Security" and specifically (under section 5.7.1) to "ICT Security", with a specific focus on capacity building.

Overall, the Guidelines seem to be limited in terms of linkages with other policy documents significant for digital security policy (e.g. Cyber Security Strategy), indicating that digital security in Latvia considered primarily as a national security issue. This perception is not unique to Latvia. In many OECD countries, the different building blocks of digital strategies operate in silos, with little co-ordination across vertical fields.

Cyber Security Strategy

The main digital security policy initiative in Latvia is the *Cyber Security Strategy of Latvia (2019-2022)*, which replaces the *Cyber Security Strategy of Latvia (2014-2018)*.

The overarching goal of the former strategy was to achieve "a secure, open, free and reliable cyberspace that guarantees the safe, reliable and continuous supply of services essential for the state and society".

The strategy applied to the government, including national and municipal administrations, the private sector and individuals. It relied on four principles (development, co-operation, responsibility and openness) and five key areas of action:

- governance of national, state-owned and critical ICT infrastructure
- the promotion of rule of law in cyber space and the reduction of cybercrime
- crisis management
- education, awareness raising and research
- international co-operation.

The new strategy (2019-2022) seems to differ slightly reflecting lessons learned over the past few years. While its vision begins in the same way (the goal is to achieve "a secure, open, free and reliable cyberspace that guarantees the safe, reliable and continuous supply of services essential to the state and society"), it also takes into account the need to respect "individual's human rights in a physical and virtual environment". This is a positive evolution that acknowledges the competing goals often at stake when devising digital security policy (e.g. privacy and national security). The new strategy also recognises the development of cyber-physical systems, and the need to move beyond the virtual-physical dichotomy.

Regarding the key areas of action, the last four are essentially the same, with the exception of "crisis management", which is now described in terms of "strengthening the resilience of ICT and provision of critical ICT and services to the public". The first key area of action has evolved from "governance" to "promotion of cyber security, reduction of digital security risks". This seems to indicate that the process of structuring the governance framework for digital security in Latvia, which was the first goal of the initial strategy, is now at least partially complete, and that the challenge for the Latvian authorities is to use this existing framework to fully engage all stakeholders in the management of digital security risk. This is a positive step, and implies that the Latvian authorities have acknowledged the need to go beyond a whole-of-government approach towards a whole-of-society approach that includes, in particular, the actors and communities involved in economic and social prosperity. This shift also implies the integration of a risk management approach. In fact, the new strategy acknowledges that ICTs "are not completely safe and can be target to attacks. The threat of an attack on ICTs cannot be completely prevented, but the risk of an attack can be greatly mitigated so as not to disrupt the economic and social development of society, to avoid economic damage and to benefit from ICTs in both public administrations and the private sector".

However, these positive changes in the new Cyber Security Strategy still need to be implemented in practice. For the Latvian government, one of the challenges will be to involve all relevant stakeholders and address digital security risks in the whole economy, with lead institutions whose primary audiences are either IT teams (CERT.LV) or the military (MoD). To be successful, a cultural shift may be needed, as well as the deeper involvement and/or support of other institutions such as VARAM, the Ministry of Economy (MoE) or the Prime Minister, whose scope is more horizontal by nature.

Other initiatives

The Latvian government has organised other initiatives in the field of digital security such as "safer internet day", "e-skills week" and "cyber security month", which aim to raise awareness and share good practices. In addition, digital security crisis exercises are carried out with public institutions, under the leadership of CERT.LV and the MoD, in accordance with the strategy.

CERT.LV has led by example with the publication of their vulnerability disclosure policy. CERT.LV accepts vulnerability reports for their own resources as well as for any other organisation in Latvia. In the latter case, CERT.LV acts as a co-ordinator among the involved parties (e.g. security researchers and organisations).

CERT.LV also provides training and information on digital security risks to IT professionals and the public. For example, it publishes regular information on online viruses and threats through its IT security portal *be safe*. The portal runs a check of each visitor's IP address against a database of infected IP addresses and informs them of any vulnerability or infection according to CERT.LV data. CERT.LV

is also engaged in educating specific professional groups including IT security officers, employees, managers, students and pupils. In 2012, CERT.LV launched the initiative Responsible Internet Service Provider (ISP), a quality label awarded to ISPs that co-operate with the team. Such co-operation includes providing incident information to end users, co-operating with the Internet Centre of the Latvian Internet Association to remove illegal material from the Internet, and providing an Internet content filter that can be set up for free on demand. Currently, Latvia has 13 "responsible ISPs", which cover approximately 77% of the Latvian Internet access market.

CERT.LV also organises educational events such as "Cyber Chess" and other knowledge-sharing activities. These events engage representatives from the private sector in digital security exercises (e.g. Kristaps and Locked Shields) which require them to solve a range of tasks together with colleagues from the public sector.

The National Guard Cyber Defence Unit (CDU) brings together experts who are interested in developing regular co-operation on digital security issues, improving expertise and knowledge at national and international level, and participating and organising training for the prevention of digital security attacks, as well as providing support to public bodies, where appropriate. The main objective of the CDU is to assist the Information Technology Security Incidents Response Institutions to prevent and respond to digital security incidents, and mitigate their consequences.

The MoD co-operates with LIKTA (the Latvian Information and Communication Technologies Association), which has 160 members, to organise among others the annual award for "the best cybersecurity initiative".

The Federation of Security and Defence Industries of Latvia (FSDI Latvia) represents the Latvian security and defence industry. At the national level, the organisation actively collaborates with the Defence Ministry, the Interior Ministry, the Foreign Ministry, the Economics Ministry and Parliament. FSDI Latvia has established the Latvian Security and Defence Cluster, which consists of small and medium companies and research institutions, as part of an EU project.

International co-operation

Latvia has developed close trilateral co-operation with its neighbouring countries Estonia and Lithuania. Policy makers from the three countries meet regularly (at least twice a year) to expand existing co-ordination, exchange information on the latest digital security trends and, in some cases, to co-ordinate a common position on digital security issues in international discussions. On a practical level, CERT.LV co-operates with Lithuanian and Estonian CERT units, exchanging information on the latest security threats, viruses and other risks, and meeting regularly in different fora. In 2015, the Estonian, Latvian and Lithuanian ministries of defence officially signed a Memorandum of Understanding on Co-operation in Cyber-security. However, there seems to a lack of co-operation among the ministries of economic affairs of the Baltic countries regarding digital security matters, even though the Estonian Ministry of Economic Affairs is the overall co-ordinator for digital security policy in Estonia (Figure 5.6).

The general manager of CERT.LV was the chair of TF-CSIRT – the European CSIRT forum – from 2014 to 2019. In this role, she supported the growth and development of the European CSIRT community, fostered collaboration in the digital security area among academia, government and public sectors, and successfully represented the European CSIRT community in different international fora.

Latvia is participating in several international training events and exercises. Examples include the three Cyber Europe exercises of the European Union Cyber Security Agency (ENISA).

Latvia is also taking part in the work of NATO, the European Union, the OSCE and the UN. It has ratified the Convention on Cyber Crime of the Council of Europe and its Additional Protocol concerning the criminalisation of racist and xenophobic acts committed through computer systems. In addition, Latvia is an active supporter of deeper co-operation among Nordic-Baltic countries, Poland and the United States.

Conclusions and policy recommendations

Latvia needs to further build upon the 2015 OECD *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*

The 2015 OECD Digital Security Risk Recommendation includes eight principles that encapsulate a "digital security risk management" approach (Box 5.1), based on the understanding that digital security is an economic and social priority as well as a technical or national security issue. This implies that:

- The overarching objective of digital security is to increase the likelihood of success of economic and social activities: digital security should be an enabler for prosperity, not an end in itself.
- Organisations cannot eliminate digital security risk altogether, but can assess and reduce risks to an acceptable level in the light of the economic and social objectives at stake.
- Digital security measures in public and private organisations can have negative effects on the economic and social activities they are expected to protect. In order to avoid this situation, leaders and decision makers in public and private organisations should integrate digital security risk management into their business decision-making processes, rather than delegating digital security risk management to technical experts. Leaders and decision makers in organisations should manage the economic opportunities and security risks stemming from the use of digital technologies in tandem.

Box 5.1. Principles of the OECD *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*

General principles

1. **Awareness, skills and empowerment**. All stakeholders should understand digital security risk and how to manage it.
2. **Responsibility**. All stakeholders should take responsibility for the management of digital security risk.
3. **Human rights and fundamental values**. All stakeholders should manage digital security risk in a transparent manner and consistently with human rights and fundamental values.
4. **Co-operation**. All stakeholders should co-operate, including across borders.

Operational principles

1. **Risk assessment and treatment cycle**. Leaders and decision makers should ensure that digital security risk is treated on the basis of continuous risk assessment.
2. **Security measures**. Leaders and decision makers should ensure that security measures are appropriate to and commensurate with the risk.
3. **Innovation**. Leaders and decision makers should ensure that innovation is considered.
4. **Preparedness and continuity**. Leaders and decision makers should ensure that a preparedness and continuity plan is adopted.

Source: OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity*, *www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf*.

Latvia has made significant steps towards the implementation of this Recommendation with the recognition of digital security as a public policy issue requiring a whole-of-government approach in the *Cyber Security Strategy of Latvia (2014-2018)* and in the *Information Society Development Guidelines*. In addition, the Cyber Security Strategy of Latvia (2019-2022) recognises the importance of a risk management approach, and acknowledges that trade-offs need to be made to implement an effective strategy for digital security, noting that while digital security measures aim to promote trust, they can

also undermine confidence. In fact, such measures may conflict with, or be perceived as conflicting with, human rights and fundamental values, in particular privacy and freedom of expression. Digital security and human rights can reinforce or undermine each other depending on how they are managed. In addition, although digital security measures aim to protect economic and social activities, they can also inhibit them by increasing costs, reducing performance and, most importantly, reducing the open and dynamic nature of the digital environment, which is essential to realising the full benefits of the digital transformation.

The above analysis of Latvia's governance structure and initiatives for digital security highlighted a strong adherence to the majority of the principles of the OECD Recommendation. However, implementation of the Co-operation, Responsibility and Innovation principles remains incomplete. If digital security is perceived mainly as a technical or a national security issue, then risk ownership and interactions between business leaders and decision makers from the private sector as well as civil society, and the institution in charge of digital security, will likely be limited. Institutions in charge of national security are also less likely to promote transparency and horizontal co-operation, and to manage programmes related to digital security innovation, SMEs and start-ups.

More importantly, the Latvian approach emphasises technology, law enforcement and national security, but pays less attention to the economic and social dimensions (Figure 5.3). Although the *Cyber Security Strategy of Latvia (2019-2022)* seems to better integrate human rights and fundamental values, as well as risk assessment and treatment, the economic and social perspective seems under developed. This may limit the ability of the government and organisations to appropriately assess risks, raise awareness and empower all stakeholders to assume their fair share of responsibility. The following areas, in particular, could be developed further: programmes to better incentivise economic actors to take appropriate security measures (e.g. certification, multi-stakeholder partnerships); sectoral and cross-sectoral initiatives to promote digital security, for instance through information sharing initiatives (ISACs); and programmes related to digital security innovation and connecting relevant stakeholders (e.g. entrepreneurs, researchers, businesses, governments, etc.).

The obstacles to enhancing digital security in Latvia identified in the *Information Society Development Guidelines* (VARAM, 2014) are approximately the same as those identified in 2016 in the mid-term review for implementation of the first *Cyber Security Strategy* (MoD, 2016). They include a lack of human and financial resources for institutions in charge of digital security; a lack of digital security skills in Latvia; and a lack of ownership of digital security risks by stakeholders, in particular senior leadership, such as decision makers and business leaders. As long as digital security is approached and perceived primarily as a technical and national security issue, and not as an enabler of economic and social prosperity, it will be difficult for Latvian authorities to generate awareness in a meaningful manner and to truly empower users and communities. In Estonia, for instance, the fundamental principles of their Cyber Strategy recognise digital security as "an enabler" of economic growth, and cite transparency and open communication as core values (MoEAC, 2019).

Latvia needs to build upon its strengths to step up its digital security policy framework

CERT.LV and the MoD have emerged as key actors in the digital security policy framework. However, other institutions in Latvia have not yet deployed a similar level of commitment in terms of human and financial resources dedicated to digital security. This could prevent these institutions from being fully involved in the design and implementation of Latvia's digital security strategy.

To bridge this gap, other institutions in Latvia should develop their own capabilities for and approaches to digital security. CERT.LV and the MoD could help build such capacity, for instance through common workshops, upskilling seminars and temporary staff sharing.

The roles of CERT.LV and the NITSC need to be enhanced

In recent years, CERT.LV has emerged as a trusted institution able to support the private sector, including Latvian SMEs, in the event of security incidents. While the NITSC has been described in the *Cyber Security Strategy* as the "central national authority for the exchange of information and co-operation between the public and private sector", it seems that CERT.LV is actually at the core

of multi-stakeholder co-operation in Latvia. Beyond its linkage with the private sector, CERT.LV has built strong connections with civil society and the technical community, as demonstrated by its interactions with the IT Security Expert Group and the Cyber Chess annual conference. The role of CERT.LV has also been instrumental in recent policy developments at the European Union level as well as within the broader CERT community, for instance regarding the responsible disclosure of vulnerabilities. However, the main audience of CERT.LV remains IT teams within public and private organisations. One of the challenges ahead for Latvia is to move ownership of digital security risk from these IT teams to the boardroom.

Latvia could leverage the success of CERT.LV to better educate and involve other ministries in the implementation of the digital security strategy, for instance through sharing staff and co-organising events and workshops.

As discussed above, the creation of the NITSC was an important step in building a whole-of-government approach for digital security; however, some shortcomings have been identified. The role of the NITSC remains unclear: it is alternately defined as an intragovernmental co-ordination body; a consultative group for the MoD, an authority in charge of designing, implementing, monitoring and evaluating the *Cyber Security Strategy*; and a gateway between the government and other stakeholders. While the current high-level format of the NITSC has enabled Latvia to step up digital security as a key public policy issue, it may also limit the ability of its members to fully leverage the issue for meaningful exchange and co-ordination. The risk is that the NITSC may become a monolithic structure where officials discuss initiatives without truly addressing key policy issues.

Different avenues could be explored to fully leverage the potential of the NITSC:

- Increase the frequency of meetings, for instance by a working-level meeting, as a complement to the high-level meeting, focused on addressing key policy issues and delivering results in a more agile manner.
- Better engage with other stakeholder groups, with the support of CERT.LV. Use a "forum" format to allow business leaders to discuss freely the challenges they face in terms of digital security on a regular, rather than an ad-hoc, basis.
- Meet once or twice a year under the leadership of the Prime Minister's office. This would indicate clearly that digital security is not solely a national security issue, but rather one that pertains to economic and social activities.

Latvia needs to better integrate an economic and social policy dimension into its governance framework for digital security

The digital security policy framework in Latvia combines a strong technical dimension (CERT.LV) with a strategic dimension (NITSC), but lacks a policy dimension that encompasses economic and social perspectives. The following avenues could be explored to address this gap:

- Increase whole-of-government engagement and co-ordination, with clear mandates and plans for "horizontal" ministries (e.g. the MoE and VARAM) to design and implement policies focused on the economic and social dimensions of digital security (sectoral partnerships, innovation, certification, etc.)
- Better integrate the *Cyber Security Strategy* with the *Information Society Development Guidelines*.
- Reinforce the *Cyber Security Strategy*'s action plan, with measurable goals oriented towards economic and social prosperity.
- Develop trilateral co-operation with Latvia's neighbouring countries Estonia Lithuania. At present, such co-operation on digital security policy exists only between CERT.LV and the MoD. A new work stream could be established linking Baltic ministries in charge of economic affairs, to discuss digital security from an economic and social perspective. (In fact, the Ministry of Economic Affairs is responsible for co-ordinating digital security policy in Estonia.) Policy makers from the three countries could meet regularly (at least twice a year) to expand co-ordination and exchange information on the linkages between digital security and economic and social prosperity.

Box 5.2. Policy recommendations

Latvia can build on existing solid foundations to address the challenges and opportunities of digital security. The Latvian Computer Emergency Response Team (CERT.LV) is recognised internationally for its technical expertise, and has led by example in regard to the adoption of co-ordinated vulnerability disclosure policies. The Latvian Ministry of Defence (MoD) is also strongly committed to promoting digital security as a strategic issue, as evidenced in the recently adopted *Cyber Security Strategy of Latvia (2019-2022)*. Most importantly, the *Cyber Security Strategy* rightly recognises digital security as economic and social risk management challenge, rather than just a technical issue. The creation in 2011 of the Latvian National Information Technology Security Council (NITSC) was a good first step towards building a whole-of-government approach to digital security.

However, public policies and the governance framework for digital security in Latvia do not yet sufficiently reflect this economic and social risk management approach. Furthermore, the design and implementation of digital security policy in Latvia are still focused on a national security framework. As a consequence, the economic and social dimensions of digital security are not sufficiently addressed in organisations and public policies (e.g. skills, innovation, SMEs). In addition, stakeholders are not consulted sufficiently in digital security policy making. To tackle these issues, Latvia should consider:

- supporting its digital security strategy at the highest level of government
- reinforcing its whole-of-government approach to digital security, by stepping up the involvement of "horizontal" ministries (e.g. in charge of economic and regional development) in digital security policy making and initiatives
- better integrating the digital security strategy with the national digital strategy (*Information Society Development Guidelines*)
- establishing upskilling and workforce-sharing programmes between public institutions, so that other ministries can benefit from the experience of CERT.LV and the MoD, as well as promoting digital security career paths
- encouraging the establishment of a multi-stakeholder community and increasing multi-stakeholder co-operation through trust-based and sustainable partnerships, (e.g. extending the role of the NITSC by organising "forum" format events to effectively engage the community)
- increasing international co-operation, in particular with other Baltic countries, in the area of digital security for economic and social prosperity, in addition to existing programmes in the areas of national security or IT security.

Developing trust through greater privacy

The General Data Protection Regulation (GDPR) provides the main legislative framework for personal data protection in Latvia as well as in another EU countries. The Personal Data Processing Law (PDPL) was adopted to regulate certain issues concerning the direct application of the GDPR in Latvia, such as determining the status of a supervisory authority and national requirements in specific situations of personal data processing.

Adoption of the PDPL took into consideration the GDPR, and thus covers the basic principles of the *OECD Privacy Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. All controllers, whether public or private, must comply with the requirements mentioned in the PDPL.

This section reviews the main features of the PDPL and its implementation. It takes into account potential challenges that have emerged in the context of the GDPR, and the main activities of the supervisory authority under the PDPL and the GDPR.

Legal framework on data protection

The PDPL along with the GDPR and the Law on the Processing of Personal Data in Criminal and Administrative Offenses constitute the current legal framework governing the processing of personal data for the public and private sector in Latvia. The PDPL is divided into 8 chapters and contains

37 sections and 5 transitional provisions. The PDPL entered in full force on 5 July 2018 and was accompanied shortly thereafter by Cabinet Regulation No. 478, entitled "Regulations regarding the Selection of the Candidates for the Office of the Director of the Data State Inspectorate and the Removal of the Director from the Office", which entered in force 18 October 2019.

A number of other laws govern privacy and the processing of personal information in different fields in Latvia. These include the following:

- The **Law on Operation of the Schengen Information System** determines which institutions have access to this system, and mandates the DSI to supervise personal data processing within this system.
- The **Electronic Documents Law** determines the legal status of electronic commerce and electronic signatures, as well as provisions for the storage of electronic documents and rules for the accreditation and supervision of certification service providers and trusted certification service providers.
- The **Electronic Communications Law** mandates the Data State Inspectorate (DSI) to supervise the protection of personal data in the electronic communications sector in accordance with rights specified under the PDPL.
- The **Human Genome Research Law** determines the supervisory functions of the DSI regarding genetic data, including the treatment of complaints regarding genetic data processing that data subjects can submit to the DSI.
- The **Law on the Security of Information Technologies** stipulates the activities that should be conducted in the event of an information security incident.
- The **Law on the Rights of Patients** determines patients' rights and protections, including personal data protection.
- The **Latvian Administrative Violations Code**, which is due to expire on 1 July 2020, determines the sanctions (and their extent) that can be imposed in cases of personal data protection breaches, as well as the procedures to impose such sanctions.
- The **Administrative Procedure Law** applies to administrative procedures in institutions whenever other laws do not provide specific rules.
- The **Criminal Law** determines criminal liability regarding personal data breaches. If the DSI concludes that a case could imply criminal liability, it may forward the case to the State Police.
- The **Law on Protection of Children's Rights** governs the prohibition on disseminating information about children, such as personally obtained information on child victims or witnesses, or children that have committed a violation of the law.

Separate regulations also prescribe technical and organisational measures for the protection of personal data.

CM Regulation 117/2004 regarding the Manner of Appraisal of Electronic Records, Procedures for the Storage thereof and Transfer to the State Archives for Storage prescribes the manner of appraisal of electronic records, the procedures for the storage thereof, and the time periods for the transfer of such records to state archives for storage. The regulation applies to state and local government institutions and legal persons, which pursuant to regulatory enactments shall transfer electronic records for state storage.

CM Regulation 473/2005 provides additional procedures for developing, preparing, storing and circulating electronic documents at state and municipal institutions, and the procedures by which the circulation of electronic documents is carried out between state and municipal institutions or between these institutions and natural persons and legal persons.

Institutional oversight

The Data State Inspectorate (DSI) was established on 2 January 2001 and operated in accordance with the former Personal Data Protection Law (expired 5 July 2018). The DSI now operates in accordance with the PDPL, the GDPR, the Law on the Processing of Personal Data in Criminal and Administrative Offenses and Cabinet Regulation No. 478 of 18 October 2019.

The DSI employs 25 people and had a reported budget of EUR 640 998 in 2019. Given the breadth of its responsibilities since the enactment of the PDPL and GDPR, staffing and resources need to be increased.

In particular, the DSI lacks sufficient resources to hire dedicated IT and technical staff to investigate privacy violations in the digital space.

The DSI also supervises the national component of the Schengen Information System, verifying that the rights of data subjects are not infringed in the processing of personal data, and represents the Republic of Latvia in the Schengen Information System Joint Supervisory Authority, the Europol Joint Supervisory Authority, the Europol Appeals Committee and the Joint Supervisory Authority of the Customs Information System, the European Data Protection Board and the Advisory Committee of the Council of Europe on the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108), as well as other actions of the European Union and international data protection authorities (DPAs).

The next sections examine the degree to which the DSI is effective at implementing the PDPL and the GDPR, and analyses available statistics related to monitoring and evaluation of the DSI's activities.

Aim and reach of the Data State Inspectorate (DSI)

Pursuant to the PDPL, the objective of the DSI is to protect fundamental human rights and freedoms in the area of data protection. The DSI conducts its activities and functioning on an independent basis taking into account the principles of equality before the law, presumption of innocence, veracity and lawfulness.

The specific activities and tasks of the DSI (in addition to those listed in Article 57 of the GDPR) are contained in Section 4 of the PDPL (Box 5.3).

Box 5.3. Main regulatory powers and activities of Latvia's DSI under the PDPL

1. Supervise the conformity of processing of personal data to the requirements of laws and regulations.
2. Promote efficiency of data protection.
3. Ensure data protection certification procedures.
4. Ensure qualification check of data protection officers and maintain a list of the data protection officers who have passed the qualification examination.
5. Provide recommendations to the the Cabinet (Saeima), local governments and other institutions according to its competence with regard to amending of laws and regulations, as well as participate in the development and opinion of draft laws and regulations prepared by other institutions.
6. Provide opinions on the conformity of data processing systems to be created in the State administration institutions to the requirements of laws and regulations.
7. Provide opinions to the national accreditation body on the conformity of the certification body pursuant to the Data Protection Regulation.
8. Co-operate with foreign supervisory authorities engaged in data protection, openness of and access to information, and unsolicited commercial communication.
9. Ensure that information requests from data subject are forwarded to the European Judicial Cooperation Unit (Eurojust) and European Police Office (Europol).
10. Represent the Republic of Latvia in international organisations and events in the area of data protection.
11. Conduct studies, analysis, provide recommendations and opinions, as well as inform the public of current issues in the areas of its competence.
12. Perform tasks set forth in other laws and regulations.
13. Publish information on its website regarding violations of the requirements of the Data Protection Regulation committed by legal persons, public and private institutions and officials, as well as other public institutions, and its elimination.

Other main obligations of the DSI under the PDPL and the GDPR include the elaboration of an annual report on its operation and functioning, which is submitted to the Saeima, the Cabinet, the Supreme Court, the European Commission and the European Data Protection Board (by 1 March), and made available on its website (Section 13).

Likewise, Section 5 of the PDPL (in addition to the rights contained in Article 58 of the GDPR), provides to the DSI a list of rights and powers to enforce the PDPL (Box 5.4).

Box 5.4. Rights of the DSI under the PDPL

1. To conduct inspection of data processing following the requirements contained in laws and regulations.
2. To draw up reports on administrative violations, examine administrative violation matters and impose administrative sanctions for violations.
3. To request and receive documents, copies and other materials necessary for the inspection, including information of limited accessibility free of charge from private persons, State administration institutions and government officials.
4. To visit State administration institutions and production facilities, warehouses, commercial and other non-residential premises owned, possessed or used by legal and natural persons in the territory of Latvia in order to verify conformity of the operation of the controller to the requirements contained in laws and regulations within the scope of its competence.
5. To become acquainted freely, according to its competence, with all types of information available in registers, information systems and databases and access it (irrespective of owner of the information) in order to obtain the information necessary for the inspection.
6. To request and receive, according to its competence, the information, documents and other materials regarding services provided to persons which are necessary for the inspection.
7. To request and receive an opinion of an independent and objective expert within the scope of the inspection.
8. To provide answers in the English language when examining complaints of non-residents in co-operation with other supervisory authorities.
9. To bring an action before courts for violations of this Law or the Data Regulation.

Pursuant to Section 6, subsection 2 of the PDPL, the Director of the DSI has the obligation to establish advisory councils, as well as working groups for the examination of issues in the areas of competence of the DSI. At the initiative of the Ministry of Justice (MoJ), the Data Protection Advisory Support Council (DPASC) was established in 2018. The aim of the DPASC is to promote the application of principles of common understanding and good governance in the implementation of the GDPR, to dispel myths and to prevent misinterpretations not only in public administration but in society as a whole.

Furthermore, the DPASC serves as a platform for discussion on matters pertaining to the GDPR and its application, sharing best practices and expertise, promoting data protection and discussing issues of mutual interest. The Council is managed by the Secretary of State of the MoJ, and comprises the DSI and representatives from the largest sectors (media, health, welfare, education, etc.).

The Latvian Association of Local and Regional Governments (LALRG) regularly organises discussions and publishes information on data protection. LALRG is a public organisation associating with local governments of the Republic of Latvia on a voluntary basis. In accordance with Article 96 of the Law on Self-Governments, the LALRG has the authority to represent local governments in negotiations with the Cabinet of Ministers, since the LALRG represents more than a half of all types of local governments. All the local governments of Latvia (9 cities and 110 municipalities) are members of the LALRG. Other institutions can also contact the MoJ and the DSI. At the beginning of 2019, data protection experts from ministries and their subordinate institutions gathered to discuss the most pressing issues in relation to implementation of the GDPR, including data protection, and to share best practices and expertise.

The PDPL contains five transitional provisions. Section 5 states that the Cabinet shall assess the effectiveness of the regulation regarding the qualification exam for data protection officers contained in the PDPL, and submit an assessment regarding the possibility of abolishing this examination to the Saeima by 30 June 2021.

Enforcement

The DSI is responsible for enforcement of the PDPL and the GDPR and other national laws governing privacy and data protection.

On 26 August 2019, the DSI imposed a financial penalty on an online retailer to the amount of EUR 7 000 for non-compliance with the GDPR, specifically for not respecting and protecting the rights to erasure of data subjects and for not co-operating with the supervisory authority. The sanctions were applied because the retailer failed to carry out its duty as a controller to execute the data subject's request and also did not provide the DSI with the requested information within the specified time period. The retailer also failed to comply with an order issued by the DSI in accordance with GDPR Article 58(2)(c) and (g) and Article 23 of the PDPL.[5]

Concerning decisions on fines, in 2019, the DSI received 1 236 complaints related to possible violations of personal data processing. In response, 246 inspections were made and fines were imposed in 9 cases. The range of fines imposed in administrative infringement cases ranged from EUR 300 to EUR 150 000. A warning was issued in seven cases.

The number of decisions taken in administrative violation cases corresponding to 2018 and 2017 is shown in Table 5.1.

Table 5.1. Decisions taken in administrative violation cases

	Decisions taken (number)	Decisions on termination of a case (number)	Penalty applied (number)	Including		Total amount of fines (EUR)
				Fine imposed (number)	Warning issues (number)	
2017	151	86	65	35	30	46 593
2018	97	71	26	12	14	10 230
2019	45	29	16	9	7	163 523

Source: DSI (2020), *Activity Report 2019, Data State Inspectorate Republic of Latvia*, *https://www.dvi.gov.lv/en/wp-content/uploads/2013/01/Annual-report-2019.pdf*.

Likewise, the DSI reports that out of 20 challenged decisions of the Inspectorate officials regarding administrative violation, 12 were appealed to the court. In total, 24 court proceedings were initiated in 2018. The DSI reports that the number of cases appealed to the court decreased in 2018, as 3 fewer challenged Inspectorate decisions were appealed than during 2017.

Technical measures for data protection

The PDPL does not contain any specific provisions or sections dealing with technical and organisational security measures of personal information. Article 32 of the GDPR establishes the obligation of controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Section 68(1) of the Electronic Communications Law of Latvia contains a provision on the security of processing of personal data for providers of electronic communications, which mandates that said providers: 1) ensure that personal data can be accessed only by authorised staff and used for previously specified purposes; 2) ensure that personal data are protected against accidental or unlawful destruction or accidental loss, and unauthorised or unlawful storage, processing, access or disclosure; and 3) document the internal procedures for the investigation and prevention of breach of personal data protection.

Personal data breach notification

Article 33 of the GDPR establishes that the controller shall notify security incidents or data breaches of personal information to the supervisory authority without undue delay and no later than 72 hours after become aware of the situation when the data breach represents a risk to the rights and freedoms of individuals. Article 34 of the GDPR establishes the obligation of data controllers to communicate data breaches of personal information to the data subject without undue delay when the data breach is likely to result in a high risk to the rights and freedoms of natural persons.

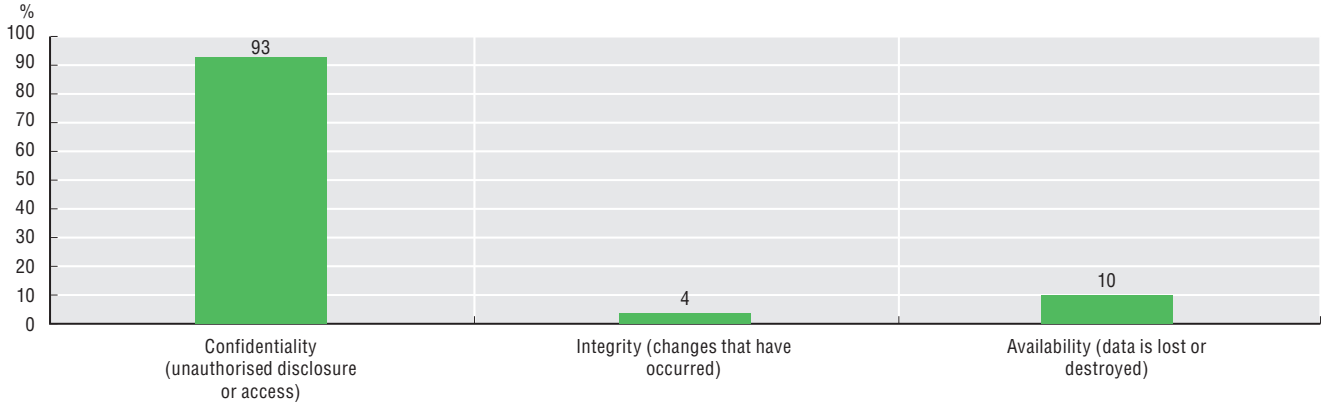
Activities that should be performed in the event of a data breach are established under the GDPR and the Law on the Processing of Personal Data in Criminal and Administrative Offenses. The GDPR and the *Guidelines on Personal data breach notification under Regulation 2016/679* regulate obligations on data breach notifications for data controllers and data processors.[6]

The Law on the Security of Information Technologies prescribes the activities that should be performed in the event of information security incidents.

The main purpose of the Law on the Security of Information Technologies is to improve the security of information technologies among the state, local government authorities and private institutions. The law establishes obligations to notify security incidents and actions to prevent security vulnerabilities. Section 6(2) stipulates that state or local government institutions or the possessor of CIITs shall within 90 days conduct all the actions necessary to eliminate the security vulnerability and inform the competent incident response institutions. Further, pursuant to section 7(4), the Security Incidents Response Institution may be allowed to perform processing of personal data that is not related to the prevention of such incidents, only if it prepares and sends the DSI a description of the planned processing and protection of personal data. The Security Incidents Response Institution shall prepare and submit to the DSI a report on the processing of personal data performed during the previous year by the end of January the following year.

The DSI's 2019 Annual Report reports that the DSI received 1 236 complaints and applications related to alleged breaches in the processing of personal data. The applications and complaints under Article 57 of the GDPR were submitted by both data subjects and other public authorities (most often law enforcement authorities), as well as organisations and associations. The DSI received 107 reports about personal data breaches, some of which contain several types of breaches (Figure 5.7).

Figure 5.7. Reported personal data breaches in Latvia



Source: DSI (2020), *Activity Report 2019*, *https://www.dvi.gov.lv/en/wp-content/uploads/2013/01/Annual-report-2019.pdf*.

Privacy management programmes

The accountability principle is one of the original eight basic principles of the 1980 Privacy Guidelines. The 2013 revision of the Privacy Guidelines included a new section, "Implementing accountability", which fleshes out the elements required of data controllers to implement the accountability principle, notably introducing the concept of "privacy management programmes" (PMPs). Under the revised

Guidelines, PMPs are the primary operational vehicle through which an organisation is expected to give practical effect to the basic principles contained in Part 2 of the Guidelines. Specifically, the added section states that a data controller should give ensure compliance with the Guidelines in respect of all personal data under its control by implementing a PMP tailored to the structure, scale, volume and sensitivity of its operations, and that provides appropriate safeguards based on privacy risk assessment including plans for responding to inquiries and incidents. In addition, the data controller should be prepared to demonstrate the operation of its PMP and provide notice, as appropriate, to authorities and data subjects where there has been a significant security breach affecting personal data. PMPs are still in an early phase of development in Europe and very few countries have adopted comprehensive guidelines and best practices for public sector institutions.[7]

On 18 December 2018, the DSI developed a *List of Processing Operations requiring data protection impact assessments* pursuant to Article 35(4) of the GDPR. The document contains a list of examples that data controllers should take into consideration when the processing of data may result in a high risk to the rights and freedoms of natural persons. The document lists 13 different possibilities when data controllers whose main place of establishment is the territory of Latvia are required to conduct a data impact assessment.

The DSI has also published several recommendations (e.g. on commercial communications and personal data processing in social networks). The DSI works closely with associations to develop specific guidelines for personal data processing in different fields.[8]

Policy making

NGOs can participate in policy making by commenting on draft legislation shared with the public for comments during the drafting process. NGOs are consulted before each new initiative and draft law proposal, mostly based on the invitation of the MoJ, who leads the drafting of legal acts in the area of privacy. Important NGOs include the Association of Data Protection Officials, the Latvian Information and Communications Technology Association and the Finance Latvia Association. For example, the CM regulation on the certification and supervision of credit information bureaus was elaborated in consultation with the Finance Latvia Association and the Association for Certified Personal Data Officers. Another example is the development of annual recommendations by the DSI in co-ordination with NGOs, including private actors, such as the recommendation on "Personal data processing within online social networking services", which was elaborated after the analysis of opinions of different social network service providers.

The DSI 2018 Annual Report states that the DSI has supported the development of guidelines for the protection of personal data applicable to associations of different sectors. For example, it mentions that the DSI worked on the development of guidelines on data protection with Finance Latvia Association and the Latvian Association for People Management, and also provided support to the Latvian Council of Sworn Advocates in the preparation of another set of guidelines for data protection.

Cross-border enforcement co-operation

Section IV of the *2013 OECD Revised Privacy Guidelines* highlights the importance of cross-border co-operation in the enforcement of privacy laws and the facilitation of mutual legal assistance among privacy enforcement authorities.

Articles 61 and 62 of the GDPR underline the obligation of supervisory authorities to provide mutual and effective co-operation concerning consultations, inspections and investigations regarding data protection, and establishes the criteria needed to conduct joint investigations and joint enforcement measures against controllers and data processors located in more than one member state of the European Union, respectively.

Until 2016, the DSI co-operated with foreign DPAs on a case-by-case basis and on a regular basis with other Baltic States. Following the adoption of the GDPR, the DSI co-operates with the DPAs of the EU countries on a regular basis in accordance with the GDPR.

The DSI 2018 Annual Report notes that on 15 June 2017, the DSI signed a Memorandum of Co-operation regarding the introduction of the Consult First principle, which promotes a customer-oriented focus in national regulatory activities. In applying the Consult First principle, the DSI has encouraged the controller to fulfil their duties laid down in the GDPR in 179 cases. The report provides that controllers have complied with the DSI's encouragement in 25 cases (78%).

Latvia is not yet part of the Global Privacy Enforcement Network (GPEN) or similar international networks for the enforcement of privacy and data protection laws.

Latvia ratified the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) on 30 May 2001 and its Additional Protocol Regarding Supervisory Authorities and Transborder Data Flows on 21 November 2017, respectively. Latvia signed the Protocol amending Convention 108 (Convention 108+) on 10 October 2018 but has not proceeded with ratification.

The DSI 2018 Annual Report states that the DSI continues to participate in the work of the Advisory Committee of the Council of Europe's Convention 108 by participating in meetings, providing the required statistical information and commenting on prepared working documents.

Monitoring

The DSI produces an annual report and submits a summary of the report to the MoJ. This report details the DSI's main activities, provides information on financial resources and staff and a summary of court cases, as well as information on the main issues that occurred over the year. It also outlines the DSI's priorities for the coming year. In accordance with the relevant CM regulation, the annual reports and their summaries are available (in Latvian) on the website of the DSI.

Complaints received by the DSI are analysed quarterly and addressed according to the planned priorities of the DSI for the current year. In some cases, complaints are analysed on a. more ad-hoc basis, for example if the DSI receives several complaints on the same matter within a short period of time.

Education and awareness

The DSI 2018 Annual Report states that the DSI in co-operation with the MoJ has developed information materials for the population on the scope of application of the GDPR. Known as "Myths and Truth", these which explain to national citizens their rights, as well as the duties of controllers and data processors under the GDPR. The DSI organised 52 lectures and seminars on the protection of personal data and the application of the GDPR to representatives of the public and private sector, and attended 76 seminars, conferences, discussion meetings and working parties organised by other institutions and economic operators.

Data governance frameworks

Access to and sharing of data is crucial for innovation in the digital economy. For example, access to data can enhance public service delivery and facilitate the identification of emerging governmental and social challenges.

The management of the Open Data Policy is co-ordinated by the Government of Latvia.

The Latvian Open Data Portal was created by the European Regional Development Fund with the support of the Public Administration Information and Communication Technology Architecture Management System (PIKTAPS).[9]

Latvia is part of the Open Government Partnership (OGP) and, as mentioned on the Latvian Open Data Portal, *The Third Action Plan for Open Government Partnership of Latvia* encompasses action to promote openness, responsibility, public participation and the use of ICTs. This plan involves actions to improve and implement various online services. One of the 12 commitments is the development of an open source public data portal. However, in order to reach the targets of 2017-2019 OGP plan, Latvia has committed to involving society in the selection of datasets. Accordingly, the website therefore has a function allowing users to vote on data they want opened up.

Conclusions and policy recommendations

Latvia has made significant progress in the enforcement of privacy and data protection rights since the enactment of the GDPR and the PDPL. The DSI has started to enforce legal frameworks in a proactive fashion and to levy administrative fines against organisations for non-compliance with the general obligations set forth in the laws. However, the DSI should be provided with the human and financial resources necessary to effectively perform its tasks, which include advising and investigating privacy and data protection in the digital space.

The 2013 revision of the OECD Privacy Guidelines introduced the concept of PMPs which serve as the core operational mechanisms through which organisations implement privacy protection. Specifically, Paragraph 15(a)(i) specifies that a data controller's PMP should put into effect the OECD Privacy Guidelines "for all personal data under its control". The development of guidance by Advisory Committee of the Council of Europe's Convention 108 the DSI to more proactively enforce the provisions of the GDPR on privacy by design and privacy by default, as well as on PMPs, is pending and should take into account the guidelines developed by the EDPB as well as existing best practices in OECD countries.

Concerning accountability obligations, the DSI has developed a list of processing operations requiring privacy impact assessments. However, the DSI still needs to further develop guidelines for accountability obligations set forth under the GDPR, such as adherence to codes of conduct and promoting the use of existing certification schemes following the developments in this area across OECD countries. At the time of writing, the DSI also needed to put in place examinations for data protection officers.

Regarding international co-operation, the DSI has been quite active in the European context, particularly in terms of its participation in the Data Protection Board (EDPB) and the Advisory Committee of the Council of Europe's Convention 108. The DSI, however, has not yet joined the Global Privacy Enforcement Network (GPEN), which could facilitate and enhance its co-operation with other countries and regions.

A clear distinction between the use and processing of special categories of data and the protection of privacy rights remains a particular task that deserves special attention in the context of AI and the development of the IoT. The DSI should thus ensure that the rights of data subjects continue to be enforced under the GDPR and the national data protection legal framework. Further safeguards that help to improve the protection of data subject rights in the context of AI and the IoT remain tasks to be further developed. This could be achieved through further participation in and collaboration with international fora on data protection and privacy including the work of the OECD in these fields.

Box 5.5. Policy recommendations

Latvia should take further steps to enhance privacy by:

- providing the Data State Inspectorate (DSI) with the human and financial resources necessary to perform effectively its tasks, including advising and investigating privacy and data protection in the digital space
- encouraging the development by the DSI of guidance based on existing good practice to promote accountability as well as "privacy management programmes" (PMPs)
- encouraging co-operation between the DSI and other countries, including outside the European Union, for example by joining the Global Privacy Enforcement Network (GPEN)
- establishing appropriate governance of AI and the IoT, including through further participation and collaboration with international fora such as the OECD.

Consumer protection

Policy framework

Latvia's Consumer Rights Protection Law[10] and Unfair Commercial Practices Prohibition Law[11] contain general principles covering: 1) information disclosures; 2) product safety; and 3) unfair, misleading and aggressive commercial practices, which apply to both traditional and e-commerce transactions.

Consistent with the European Union's (EU) Consumer Rights Directive 2011/83/EU, the Consumer Rights Protection Law was amended in 2014 by a Regulation Regarding Distance Contracts,[12] which identifies key pre-contractual information disclosure requirements (regarding the business, product and transaction). The Regulation also covers the conditions for confirming distance contracts which, under Article 17, shall be provided to consumers via a durable medium and within a reasonable time after the conclusion of the contract (at the latest at the time of the delivery of the goods or before the performance of the service). The Regulation also introduces a new right of withdrawal for consumers engaging in distance contracts (including via e-commerce).

In addition to the above laws, specific e-commerce provisions are contained in the Law on Information Society Services,[13] the Electronic Communication Law[14] and the aforementioned Unfair Commercial Practices Prohibition Law.

- The **Law on Information Society Services** outlines key information that service providers must provide to consumers, including pre-contractual information about the business, the product and the transaction. It also covers codes of conduct, the conditions for storing information on a terminal equipment, requirements regarding commercial communications, liability, and the role and responsibilities of supervisory bodies, such as Latvia's Consumer Right Protection Centre and the DSI.[15] Article 4 of the law identifies general information to be provided by service providers. Article 5 lays down information to be provided by the service provider before placing the order. Article 7 specifies information about the contract terms and codes of conduct to be provided by the service provider.
- The **Electronic Communication Law** covers the rights and obligations of users, electronic communications providers, owners of private electronic communication networks and state administrative institutions, which are associated with the regulation of the electronic communication sector. It also contains provisions on electronic communications services and the use and administration of scarce resources, including spectrum allocation and assignment of radio frequencies. Furthermore, the law sets forth the rights and obligations of the respective regulatory agencies in the different sectors under regulation. It lays out specific obligations applying to entities and businesses with significant market power, obligations on universal services, data protection obligations for the electronic communications sector, and obligations to retain data in the provision of voice telephony, public telephony and the provision of public Internet access services.
- The **Unfair Commercial Practices Prohibition Law** also covers online advertising targeting children, misleading and unfair commercial practices, and product safety.

Additional requirements governing online transactions and, in particular, advertising to children are provided in the Advertising Law[16] (Section 5), which sets out penalties for non-compliance with the law and secondary regulation.

Payment services, electronic money and payment cards are regulated by the Law on Payment Services and Electronic Money,[17] which establishes the rights and obligations of payment service providers and users, and e-money issuers and holders, as well as the requirements for providing payment services for issuing, distributing and redeeming e-money, and the responsibility of both payment institutions and e-money institutions.

Furthermore, Latvia is currently in the process of implementing further policies on consumer protection, consistent with recently adopted EU regulations seeking to promote and improve the European digital single market, including the European Union's Regulation on geo-blocking.[18] Following the entry into force of the European Union's Regulation[19] on co-operation between national authorities responsible for the enforcement of consumer protection laws, amendments to Latvia's Electronic Communications Law were adopted in 2018, which provide the national Consumer Rights Protection Centre (CRPC) with additional powers to request information from electronic communications providers regarding information on the subscriber or user (e.g. webmaster).

Implementation of OECD principles on the protection of digital consumers

This section aims to evaluate the degree to which Latvia's consumer policy framework incorporates general principles for protecting digital consumers, consistent with the OECD *Recommendation of the Council on Consumer Protection in E-commerce*, otherwise known as "the E-commerce Recommendation" (OECD, 2016). The Recommendation's key provisions are contained in Box 5.6. The section also examines

the degree to which Latvia's framework covers the wide variety of forms that e-commerce now takes, including transactions between consumers, transactions via mobile devices and transactions that do not involve a monetary payment.

Box 5.6. General principles for protecting digital consumers

The OECD *Recommendation of the Council on Consumer Protection in E-commerce* sets the key provisions for the protection of digital consumers:

- fair business and advertising practices
- appropriate disclosures
- effective processes for transaction confirmation and payment
- product safety across e-commerce supply chains
- meaningful access to effective mechanisms to resolve disputes
- consumer education and awareness
- authorities' powers to investigate and take action at domestic level
- authorities' ability to engage in international policy and enforcement co-operation.

Source: OECD (2016), *Consumer Protection in E-commerce: OECD Recommendation*, *www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf*.

The E-commerce Recommendation was revised in 2016 to cover a number of new issues and developments, such as the rapid growth and consumer adoption of intangible digital content products, changing and more active consumer behaviour online including through mobile devices, the emergence of a wide range of online and mobile payments, and growing concerns over online product safety. The Recommendation also highlights the need to provide redress to consumers involved in non-monetary transactions, and calls on businesses to provide consumers with clear and conspicuous information on the limitations, functionality and interoperability of digital content products, and to address the privacy and security risks of e-commerce services including payment methods.

Institutional oversight

The E-commerce Recommendation contains updated provisions on the essential role of consumer protection enforcement authorities (CPEAs) and the need to enhance their ability to protect consumers in e-commerce. Part 2 of the Recommendation outlines implementation principles for the regulatory framework, and calls on governments, in co-operation with stakeholders, to achieve the purpose of the Recommendation by:

- reviewing and, if necessary, adopting and adapting laws protecting consumers in e-commerce, having in mind the principle of technology neutrality (53 ii)
- establishing and maintaining CPEAs that have the authority and powers to investigate and take action to protect consumers against fraudulent, misleading or unfair commercial practices and the resources and technical expertise to exercise their powers effectively (53 iii)
- encouraging the continued development of effective co-regulatory and self-regulatory mechanisms that help to enhance trust in e-commerce, including through the promotion of effective dispute resolution mechanisms (53 v).

In Latvia, consumer policy making, implementation and enforcement related to e-commerce falls under the responsibility of the same authorities covering traditional shopping. Consumer policy making is led by the MoE,[20] specifically the Competition, Trade and Consumer Rights Division. Sector-specific policies addressing consumer issues (e.g. health services, transport or telecommunications) are covered by other ministries in co-ordination with the MoE. Given that consumer protection, including dispute resolution, is closely linked to civil and administrative law, the MoJ is also engaged in the development of consumer policy.

The main implementation and enforcement body is the CRPC,[21] under the MoE. While the MoE is responsible for reviewing the legal compliance of the decisions made by the CRPC, it may not interfere with the CRPC's decision-making process or revise an opinion upon which a decision was made. The MoE has the right to intervene and order the CRPC to take a decision, only in cases where the CRPC fails to act according to the law (unlawful failure to act). The Director of the CRPC is appointed for a term of five years by the Cabinet of Ministers on the recommendation of the MoE. In accordance with the Consumer Rights Protection Law, decisions of the CRPC may be appealed in court in accordance with the procedures specified in the Administrative Procedure Law.

The CRPC's main objective is to implement consumer rights and interests. Its responsibilities include handling individual consumer complaints, carrying out market surveillance of most non-food products, and enforcing consumer laws and regulations. Additional enforcement authorities complement the CRPC in specific areas, including the DSI, which is responsible for personal data protection, and some sector-specific ministries that have dedicated budget and staff for consumer protection.

The CRPC has broad regulatory powers (Box 5.7), including the possibility to require businesses to publish relevant information when consumer rights have been violated, for example in cases of false or misleading product information, unfair commercial practices or hazardous products.

Box 5.7. Main enforcement powers of the CRPC

- Request from businesses, the state, local government institutions and natural or legal persons all information necessary for the CRPC to fulfil its functions.
- Ask businesses to undertake voluntary actions within a prescribed period of time to ensure conformity of commercial practices with legal and regulatory requirements, such as to terminate unfair commercial practices.
- Require businesses to publish relevant information when consumer rights have been violated, for example in cases of false or misleading product information, unfair commercial practices or hazardous products.
- Visit any building, premise or places where goods that are not in compliance with consumer protection policy and law are manufactured, stored or traded, or where non-compliant services are being provided; visit any place in which measuring instruments are used, manufactured, repaired or sold.
- Request and receive samples of a good that is suspected to violate consumer rights in accordance with the procedures specified in regulatory enactments for carrying out laboratory or other expert examinations.
- Request the withdrawal of goods from circulation or terminate the provision of services, in cases of non-compliance with consumer protection policy, regulation or technical standards.
- Suspend, during an investigation, the sale of goods or the provision of services until a decision is taken based on a testing result from a laboratory or an expert opinion.
- Impose administrative sanctions and fines.

The CRPC currently has 107 staff members, most of whom are involved in consumer rights enforcement and product safety issues, including: goods and service surveillance, consumer rights protection, consumer consultations and complaints, and cross-border issues. Some consumer law enforcement is carried out by the DSI, in particular in the context of e-commerce. The supervision of e-commerce is performed by specific supervisory departments of the CRPC, with the assistance of support units. Table 5.2 provides budget and staff resource information for the period 2017-19.[22]

In addition to the CRPC, the following institutions can request and receive information, and apply administrative sanctions (fines, prohibitions): the State Health Inspectorate (advertising veterinary and pharmaceutical services) and the National Electronic Mass Media Council (advertising). The State Police may be involved in cases that involve criminal offences, for example related to spam.

Table 5.2. CRPC budget and staff, 2017-19

	Budget (EUR)	Staff (without ECC-Net)
2017	2 383 111	96
2018	2 895 983	107
2019	2 849 981	107

Source: OECD, based on data from CRPC.

The number of consumer complaints regarding distance contracts received by the CRPC has increased significantly in recent years. For example, around 486 complaints were submitted in 2017 compared to 222 in 2016, representing a more than 200% increase. The CRPC has investigated several cases and taken decisions to protect consumer interests, and has also published consumer guidance and alerts in the media to inform consumers about issues associated with specific online retailers and platforms.

Table 5.3 contains consumer complaints data submitted to the CRPC from 2017 to June 2019.

Table 5.3. Consumers complaints received and resolved by CRPC, 2017 – June 2019

	Complaints received	Complaints resolved
2017	3 616	958
2018	3 604	1 002
2019 (until 30 June)	1 940	405

Source: OECD, based on data from CRPC.

Enforcement

The CRPC regularly undertakes enforcement actions in the context of e-commerce. In addition to the regulatory powers described in Box 5.7, the CRPC can mandate the blocking of illegal content on websites that is harmful to children, including from service providers registered outside the European Union. In many cases, the CRPC's enforcement actions are related to unfair commercial practices in e-commerce.

Complaints related to criminal fraud are usually sent to the State Police for corresponding investigation and follow-up through criminal proceedings. Some of the complaints concerned online retailers failing to deliver products or reimburse customers. Table 5.4 provides complaint data received from 2017 to June 2019.

Table 5.4. Complaints related to e-commerce, 2017 – June 2019

	Businesses involved	Consumer complaints received	Resolution
2017	6 online retailers	196	Referred to the State Police
2018	3 online retailers	252	Referred to the State Police
2019 (until 30 June)	1 entertainment event	105	Referred to the State Police

Source: OECD, based on data from CRPC.

Unfair commercial practices are considered a breach of collective consumer interests and are enforced through collective actions on the part of consumers (via administrative proceedings). Individual consumer complaints may not be resolved through such collective actions, but the CRPC is competent to intervene and terminate those commercial activities in violation of consumer law. It may do so on a voluntary basis through voluntary infringement cessation or undertakings, or by issuing administrative decisions. Undertakings received from businesses and the CRPC's administrative decisions may be used as evidence by consumers who seek redress in court or engage in alternative dispute resolution. Not all consumer complaints may, however, trigger collective actions (e.g. one collective case may contain several consumer complaints, a consumer's complaint regarding infringement may not be upheld, a collective case may be underway prior to the consumer complaint, etc.).[23]

While there are no specific statistics available on unfair commercial practices in e-commerce, Table 5.5 provides complaint activity related to different types of commercial practices, some of which relate to e-commerce.

Table 5.5. Official consumer complaints related to unfair online commercial practices, 2017 – June 2019

	Complaints
2017	204
2018	279
2019 (until 30 June)	197

Source: OECD, based on data from CRPC.

Likewise, while there are no specific official statistics available on unlawful practices in e-commerce. Table 5.6 shows contains internal case handling information ("Uzraugs") stored on the internal database system of the CRPC.

Table 5.6. Unlawful e-commerce practices, 2017 – June 2019

	Administrative cases commenced	CRPC calls for voluntary cessation	Written undertakings received	Administrative decisions issued	Penalties applied (EUR)
2017	99	50	8	12	85 000
2018	177	149	1	18	194 900
2019 (until 30 June)	71	39	2	6	52 570

Note: CRPC = Consumer Rights Protection Centre.

Source: OECD, based on data from CRPC.

Monitoring and evaluation

The implementation of consumer protection in the context of e-commerce is assessed in a report submitted annually by the CRPC to the MoE.[24] The CRPC's 2018 Annual Report[25] included several interesting insights, statistics and information about enforcement actions conducted in the area of e-commerce. For instance, concerning fair pricing practices and distance contract terms from online retailers, the report indicates that "25 of the most popular internet shops were inspected and 25 administrative cases proceeded", followed by voluntary cessation of infringement.

Another useful monitoring tool is the Internet Sweep,[26] which is organised by the European Commission and the International Consumer Protection and Enforcement Network (ICPEN) as a means to enforce EU consumer protection law. Sweeps have been conducted in different areas including digital products, online airline ticket sales and online games targeting children. The results provide useful information on possible infringements of consumer protection legislation and help Latvia evaluate the seriousness of the issue, and the effectiveness of consumer policy implementation in the country.

Education and awareness

The CRPC regularly informs consumers about ways to shop safely online, both in response to questions from journalists and through social media channels. The CRPC maintains a website[27] to inform consumers about possible risks associated with misleading and fraudulent commercial practices conducted by specific online shops and platforms.

Furthermore, the CRPC has developed a checklist[28] with tips and useful information for consumers when deciding whether to buy from an online shop.

The CRPC has also distributed information (videos, gifs, infographics) provided by the Network of European Consumer Centres (ECC-Net) on subscription traps and online shopping. In 2018, the CPRC collaborated with the Patent Office on a campaign about counterfeit goods.

During 2019, the CRPC participated in an open day for government institutions.[29] High-school students visited the CRPC and participated in a variety of activities, obtained information about safe shopping online and how to recognise unsafe goods, and learned about consumer rights not only in Latvia, but also in the European Union.

The CRPC has been highly active in promoting consumer rights on social networks. In 2019, on Valentine's Day, it launched a campaign on how to choose an Internet dating website.[30] The CPRC also regularly publishes information on consumer protection rights on the Internet on its website.

In addition to educating consumers, the CRPC has engaged in the promotion of consumer rights to businesses involved in e-commerce activities. In particular, the CRPC has issued non-binding guidelines to help businesses interpret legislative acts, in particular focusing on electronic communication services markets, contractual terms and conditions in e-commerce, group buying, and notice and action procedures to obtain voluntary infringement cessation on websites.

In September 2015, the CRPC published a set of *Guidelines for Online Games Targeting Children*.[31] The authority collaborated with the European Commission and Denmark on in-app purchases, focusing on children gaming mobile applications, the results of which fed into the Guidelines.

National NGOs also play an active role in promoting consumer protection in the context of e-commerce. For example, the Latvian Internet Association[32] runs awareness-raising initiatives on Internet safety, including in the context of e-commerce. LIKTA,[33] in collaboration with the MoE, has conducted several activities such as seminars on e-commerce and e-services, organised an E-commerce Information Day and created an E-commerce Award for the best e-commerce vendor. NGOs also play an important role in implementing unfair commercial practice legislation in the context of e-commerce, by regularly informing the CRPC about possible infringements.

Furthermore, LIKTA promotes e-skills as well as awareness about the topic of online safety. Over 180 000 individuals across Latvia have participated in its training initiative Latvia@World (Latvija@Pasaule) since 2005, which offers training and certification, and has developed different training projects for e-skills and inclusion training.

Dispute resolution and redress

The objective of Latvia's policy on dispute resolution and redress (DRR) is to enable consumers to exercise their rights when entering into contracts with manufacturers, traders or service providers, and to provide consumers with access to fair and effective DRR, whether acting individually or collectively in Latvia, as well in cross-border-related disputes.

Disputes that cannot be resolved between a business and the consumer are dealt with by civil courts or through alternative dispute resolution (ADR) entities. The main ADR institutions are the CRPC and the Public Utilities Commissions (PUC), as well as private ADR organisations.

The CRPC includes a national ADR contact point and maintains a list of ADR institutions, as well as a Consumer Complaints Committee (CCC).

The CCC was established through recent amendments to the Consumer Rights Protection Law in accordance with EU Directive 2013/11/ES on alternative dispute resolution for consumer disputes. The CCC will operate under the authority of the CRPC and settle disputes between consumers and traders (businesses). The CCC will be composed of three or more committee members, representing on equal terms experts from consumer and trader NGOs with one impartial chair member.

Latvia's Law on Consumer Alternative Dispute Resolution[34] has been in force since July 2015. The law sets out rules for alternative dispute resolution entities, ensuring that consumers can issue and protect their legal rights by submitting complaints against businesses, while offering independent, impartial, transparent, effective, fast and fair alternative dispute resolution procedures. The law applies to ADR entities and procedures for out-of-court resolution of domestic and cross-border disputes concerning contractual obligations. Furthermore, the law provides specific rules and responsibilities (duties) for ADR entities and applied procedures, including a framework for co-operation among ADR

entities and between ADR entities and other institutions. The law does not apply to: 1) procedures before dispute resolution entities when the natural persons in charge of dispute resolution are employed or remunerated exclusively by the individual trader; 2) procedures before consumer complaint-handling systems operated by the trader; 3) direct negotiations between the consumer and the trader; 4) procedures initiated by a trader against a consumer; disputes between traders; disputes relating to non-economic services of general interest; 5) disputes regarding health services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices; and 6) disputes concerning public providers of further or higher education; and disputes relating to an act or negligence on the part of sworn notaries or bailiffs.

Cabinet Regulation 631/2008[35] regulates procedures for the submission and examination of consumer claims regarding the non-conformity of goods or services with contract provisions.

European Parliament and Council Regulation (EC) 861/2007[36] established a European small claims procedure, intended to reduce costs and simplify and speed up litigation concerning small claims in cross-border cases. In Latvia, claims for small amounts can be submitted in accordance with the Latvian Code of Civil Procedure,[37] which provides simplified proceedings for claims below EUR 2 100.

Implementation and enforcement

The MoE[38] plays an essential role in implementing Latvia's DRR policy, co-operating closely with other ministries and authorities, such as the State Health Inspectorate, the State Food and Veterinary Service, and the PUC, as well as with NGOs.

According to the rules on dispute resolution procedures provided in the Consumer Rights Protection Law (section 26), consumers should lodge a complaint first with the business in order to seek a direct settlement. The CRPC and other institutions provide advice to consumers about their rights in specific situations and appropriate actions to request redress. Consultations may be conducted by phone, e-mail and face-to-face at the CRPC premises. Approximately 40-45% of initial complaints can be resolved through such conciliation procedures. If direct negotiations do not produce a solution, consumers have several other options.

If a consumer files a compliant with the CRPC and no solution can be reached with the business, a dispute settlement procedure may be initiated following Cabinet of Ministers Regulation 613, through which the CRPC engages directly with the business to obtain a solution. This may include an administrative procedure and a binding decision. Such administrative procedures undertaken by state institutions do not impose any costs on consumers, and it is the duty of the responsible institution or the court – if the decision is appealed in court – to gather the necessary information and evidence resolve the dispute.

Several industries in Latvia are providing their own dispute resolution mechanisms. The CCC, which operates under the authority of the CRPC and includes private sector representation, has established an alternative dispute resolution body.

Consumer complaints are collected systematically and addressed by product category and consumer protection issue. In addition, the CRPC and other government agencies and NGOs carry out surveillance activities to analyse market trends on a regular basis. The CRPC undertakes a variety of awareness campaigns, including in co-operation with national businesses and NGOs, to help consumers deal with DRR.

The Consumer Rights Protection Law (sections 22 and 23) gives non-governmental consumer organisations the right to defend consumer interests and to participate in the decision-making process. Furthermore, in accordance with Cabinet Regulation No. 300 Rules of Procedure of the Cabinet of Ministers,[39] non-governmental stakeholders must be involved in the drafting of legislation and policy planning documents. Consumer NGOs also have the right to examine consumer complaints, assist consumers in judicial cases and represent consumer interests in national courts. The work of the NGOs is perceived as an important source of information on developments in consumer markets, including potential or actual violation of consumer rights. Table 5.7 presents statistics on consumer disputes, both domestic and cross-border.

Table 5.7. Domestic and cross-border consumer disputes

	Domestic cases			Cross-border cases ECC-Net		
	Disputes	Redress[1]	Solved[2]	Disputes	Redress[1]	Solved[2]
2017	1 929	..	595	634	..	285
2018	1 976	..	707	489	..	203
2019 (until 30 June)	1 132	..	203	235	..	172

1. Information on redress is not available for the CRPC.
2. An agreement between the parties has been reached (but not necessarily redress).

Source: CRPC.

The above information indicates that Latvia's system of data collection and analysis has improved in recent years, with the CRPC now able to distinguish between domestic fraud and cross-border cases.

Enforcement of laws against spam

The objective of Latvia's policy on spam is to promote fair commercial practices and to ensure compliance with rules for the processing of personal data in the context of commercial communications. Commercial communications include automatic calls, emails and faxes sent to individuals without their explicit consent. Rules for the processing of personal data cover the contact details that may be collected by a service provider, including in particular when such processing is conducted for purposes other than the commercial transaction for which the data were collected.

Legal framework

The general requirements regarding information to be provided by manufacturers or service providers (businesses) to consumers are stipulated in the Consumer Rights Protection Law. The Unfair Commercial Practices Prohibition Law regulates commercial practices which are misleading, aggressive or ignorant in terms of professional diligence. The Personal Data Protection Law provides principles and regulation of personal data protection, in particular the sending of unsolicited commercial messages, or spam, which may be considered a violation. The main purpose of the Law on the Security of Information Technologies[40] is to improve the security of information technologies. The law specifies the most important requirements to guarantee the receipt of essential services supplied through such technologies. It also establishes the Information Technology Security Incident Response Institution of the Republic of Latvia (CERT.LV),[41] an institution whose mandate includes the supervision and management of the security of information technologies of state and local government authorities, which may include countering spam.

More detailed rules for the protection of personal data and prohibitions on unsolicited commercial communications are established in the Law on Information Society Services. This law prohibits automated commercial communication if the recipient has not given his prior, free and explicit consent, and requires such communication to include the possibility of rejection by the recipient. These legal obligations also apply to automated calling systems that function without human intervention, including e-mail and fax. Additionally, the law establishes the conditions under which a service provider who has acquired electronic mail addresses from customers in the context of commercial transactions may use such addresses for other commercial communications. These include the following circumstances: 1) the commercial communications concern similar products or services from the service provider; 2) the client has not objected to receiving further emails; and 3) the customer has been given a clear, distinct, free-of-charge opportunity to reject further emails.

Enforcement powers

The two main institutions with responsibilities and powers related to spam are the DSI and the CRPC. Both authorities may request and receive information, enforce legal duties and impose administrative sanctions (fines and prohibitions). Furthermore, the State Police of Latvia[42] (Ministry of Interior) may become involved if the spam cases relate to criminal offences, and the CERT.LV may intervene if the cases affect the security of information systems and networks. Both businesses and NGOs related to

consumer protection contribute to the enforcement of spam legislation, including through informing the competent supervision authority about possible infringements.

If a supervisory body detects a violation of the law, it is entitled to: 1) request all information necessary to clarify the circumstances of the case; and 2) order the service provider to cease violating the law and specify a time period in which the business must comply with the law.

In order to avoid conflicts of interest, the CRPC's activities on dispute resolution are separated from its enforcement activities. Dispute resolution is handled by the Department of Consumer Consultation and Complaints and enforcement is conducted by the Department of Consumer Rights Enforcement.

Cross-border co-operation

Latvian spam enforcement authorities co-operate with foreign spam enforcement authorities, mainly within Europe. Specifically, in accordance with the Law on Information Society Services, the CRPC co-operates with authorities from European Economic Area (EEA) states. Furthermore, the DSI participates in a co-operation network for the national authorities of EU countries pursuant to EC Regulation 2006/2004[43] on co-operation between national authorities responsible for the enforcement of consumer protection laws. This co-operation is of particular relevance for spam cases that involve infringement of the Personal Data Protection Law.

There is a lack of sufficient information or evidence on the degree to which the CRPC and the DSI are evaluating the effectiveness of Latvia's spam policy and have undertaken appropriate measures and improvements, such as improved co-operation with foreign enforcement authorities outside of the EEA.

The CRPC has no specific information or statistics concerning spam or related issues and enforcement activities. Data on spam are collected by CERT.LV. Co-operation across agencies to share related information and analyse such data might help to address consumer issues in this area.

Bilateral assistance and cross-border co-operation

Cross-border fraud is mainly addressed through the CRPC's participation in several European and international networks that enhance information exchange and enforcement co-operation. The CRPC is part of the European Co-operation Network of Enforcement Agencies, which was established by the Consumer Rights Protection Law, and is used to address collective consumer cases. Latvia is also part of the ECC network (ECC-Net),[44] a Europe-wide network that helps to resolve individual cross-border disputes within the European Union. Four individuals appointed by the CRPC are currently working for the ECC network. Best practices and enforcement mechanisms are also circulated via the European Commission and the working parties of the EU Council.

Furthermore, the CRPC is a member of ICPEN and participates in EU and ICPEN sweeps to prevent cross-border infringements in different areas, such as tourism or in-app purchases. The CRPC also participates in Fraud Prevention Month, which is co-ordinated by ICPEN.

Latvia has signed several bilateral agreements to combat cross-border fraud. In particular, the CRPC has signed co-operation agreements with the Lithuanian and Estonian consumer protection and market surveillance authorities. Joint meetings are held at least once per year to share work results, discuss joint cases and share best practices. In September 2011, the CRPC also signed a Joint Declaration of Intent with the Standardization Administration of Israel's Ministry of Industry, Trade and Labour (MoITAL) to co-operate on market surveillance and enforcement in the area of non-food consumer product safety.

Latvian consumers encountering fraud involving a business based in a foreign country can file a complaint with the CRPC. If an EU cross-border infringement case is detected in Latvia, the CRPC acts according to the CPC Regulation by sending information and/or enforcement requests to other EU enforcement agencies. If the infringement has been committed by a company acting outside the European Union, the CRPC can use the ICPEN co-operation mechanism. Consumers can also file complaints on an e-consumer website,[45] a global system for co-operation on cross-border cases in which CRPC participates.

Conclusion and policy recommendations

Box 5.8 contains proposed recommendations for Latvia to improve its evidence base for consumer policy decision making, and enhance consumer protection both within and outside the European Union.

Box 5.8. OECD recommendations for Latvia to enhance consumer protection

Latvia should consider:

- Developing consumer complaints data specific to e-commerce in order to better understand the nature and scale of consumer issues associated with e-commerce transactions (consistent with the OECD E-commerce Recommendation, paragraph 53).
- Enhancing consumer awareness of issues associated with e-commerce, and improving their digital competence through awareness programmes, bearing in mind the special needs of different groups based on, for instance, their age, income and literacy (consistent with the OECD E-commerce Recommendation, paragraphs 50-51).
- Assessing the effectiveness of the country's dispute resolution and redress system by exploring, for instance, consumer usage and satisfaction as well as unresolved dispute cases.
- Improving the evidence base on cross-border disputes outside the European Union and enhancing cross-border enforcement co-operation within and outside the European Union.

References

CERT.LV (2020), *CERT.LV reģistrētie incidenti no 01.01.2020. līdz 31.03.2020* (Incidents registered with CERT.LV from 01.01.2020. until 31.03.2020), *https://cert.lv/lv/2020/04/pieejama-statistika-par-2020-gada-1-ceturksni*.

CERT.LV (2018), *CERT.LV Public Performance Report*, Ministry of Defence, Riga, *https://cert.lv/uploads/cert-gada-parskats-2019.pdf*.

DSI (2020), *Activity Report 2019*, Data State Inspectorate Republic of Latvia, Riga, *https://www.dvi.gov.lv/en/wp-content/uploads/2013/01/Annual-report-2019.pdf*.

MoD (2020), *Publiskais pārskats par CERT.LV uzdevumu izpildi: 2020. gada 1. ceturksnis* [CERT.LV Quarterly Public Review], Ministry of Defence, Riga, *https://cert.lv/uploads/parskati/CERT-LV_Q1_2020_pub.pdf*.

MoD (2019), *Cyber Security Strategy 2019-2022*, Ministry of Defence, Riga, *https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf*.

MoD (2016), *Mid-term Review of the Implementation of the 2014-2018 Cyber Strategy*, Ministry of Defence, Riga.

MoD (2014), *Cyber Security Strategy of Latvia (2014-2018)*, Ministry of Defence, Riga, *www.mod.gov.lv/sites/mod/files/document/Kiberdrosibas_strategija%20EN%20%281%29.pdf*.

MoEAC (Estonia) (2019), *Cyber Security Strategy*, Ministry of Economic Affairs and Communications, Tallinn, *www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf*.

OECD (2016), *Consumer Protection in E-commerce: OECD Recommendation*, OECD, Paris, *www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf*.

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity*, OECD, Paris, *www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf*.

OECD (2012), *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*, OECD, Paris, *www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf*.

OECD (2002), *Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security*, OECD, Paris, *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0312*.

OECD (1998), *Cryptography Policy: The Guidelines and the Issues: The OECD Cryptography Policy Guidelines and the Report on Background and Issues of Cryptography Policy*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264162426-en*.

VARAM (2014), *Information Society Development Guidelines 2014-2020*, Ministry of Environmental Protection and Regional Development, Riga *www.varam.gov.lv/eng/darbibas_veidi/e_gov/?doc=13317*.

Notes

Israel

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

1. WannaCry is a ransomware that caused significant damage to the affected organisations. Mirai infects computers with a botnet, which then performs Distributed Denial-of-Service (DDoS) attacks.
2. The first Computer Security Incident Response Team (CSIRT) in Latvia was created in 2006 and became CERT.LV in 2011.
3. Digital security policy in Latvia spans many areas, including cyber warfare (MoD), cyber crime (MoI), telecommunications (MoT), digital security of financial systems (MoF) and privacy aspects (MoJ).
4. Except for the Bank of Latvia, which has a permanent representative on the NITSC.

5. See the news section of the European Data Protection Board, available at: *https://edpb.europa.eu/news/national-news/2019/data-state-inspectorate-latvia-imposes-financial-penalty-7000-euros-against_en*. A press release from the DSI is available at: *www.dvi.gov.lv/lv/zinas/datu-valsts-inspekcija-piemero-7000-eiro-lielu-naudas-sodu-internetveikalam-par-personas-datu-apstrades-parkapumiem*.
6. Further information on data breach notification and the notification format is available at the website of the DSI: *www.dvi.gov.lv/lv/personas-datu-apstrades-aizsardzibas-parkapuma-pazinojuma-iesniegsana*.
7. Some relevant examples are the *Best Practice Guide on Privacy Management Programs (PMP)* developed by the Hong Kong (China) Office of the Privacy Commissioner for Personal Data, which outlines the requirements of privacy management programmes applicable to private and public sectors, available at: *www.pcpd.org.hk/pmp/pmp.html*. Likewise, the Personal Data Protection Commissioner of Singapore has published a Guide to Developing a Data Protection Management Programme, which was revised on July 2019 and aims to assist public and private sector organisations in complying with the *Personal Data Protection Act of 2012*, available at: *http://bit.do/fp4*. Further, the *Guidelines for Implementing a Privacy Management Program for Privacy Accountability in Manitoba's Public Sector* were drafted in accordance with the document *Getting Accountability Right with a Privacy Management Program*, published jointly by the Office of the Privacy Commissioner of Canada and the Offices of the Information and Privacy Commissioners for Alberta and British Columbia, available at: *www.ombudsman.mb.ca/uploads/document/files/privacy-management-program-guidelines-en.pdf*. The Data Protection Agency of Mexico (INAI) developed in August 2018 a set of *Guidelines for Data Protection Management Programs* for entities of the public sector that contain guidance, measures and recommendations to comply with the obligations set forth in the *General Law on Protection of Personal Data for Public Sector Entities* and the *General Guidelines on Personal Data Protection for the Public Sector*. The document is available in Spanish at: *http://inicio.inai.org.mx/SitePages/Documentos-de-Interes.aspx?a=m4*.
8. The Recommendations and Guidelines of the DSI are available at: *www.dvi.gov.lv/en/legal-acts/recommendations-and-guidelines*.
9. The purpose of data.gov.lv is to gather and circulate data collected by government institutions and organisations in one place for public use, on the basis that these data are valuable for the development of innovation. Available at: *https://data.gov.lv*.
10. See the Consumer Rights Protection Law of 18 March 1999 at: *https://likumi.lv/ta/en/id/23309-consumer-rights-protection-law*.
11. See the Unfair Commercial Practices Prohibition Law of 22 November 2007 at: *https://likumi.lv/ta/en/en/id/167759-unfair-commercial-practices-prohibition-law*.
12. See Regulation No. 255 Regarding Distance Contracts of 20 May 2014 at: *https://likumi.lv/ta/en/en/id/266462-regulations-regarding-distance-contracts*.
13. See the Law On Information Society Services of 4 November 2004 at: *https://likumi.lv/ta/en/en/id/96619-law-on-information-society-services*.
14. See the Electronic Communications Law of 28 October 2004 at: *https://likumi.lv/ta/en/id/96611-electronic-communications-law*.
15. Available at: *www.dvi.gov.lv/en*.
16. See the Advertising Law of 20 December 1999 at: *https://likumi.lv/ta/en/en/id/163-advertising-law*.
17. See the Law on Payment Services and Electronic Money at: *www.fktk.lv/texts_files/0_Law_Payment_Services_Electronic_Money.pdf*.
18. See Regulation (EU) 2018/302 of the European Parliament and of the Council on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market at: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0302*.
19. See the Regulation (EU) 2018/302 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No. 2006/2004 at: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32017R2394*.
20. More information is available at: *www.em.gov.lv/en*.
21. More information on the CRPC is available at: *www.ptac.gov.lv/en/content/about-crpc*.
22. Available at: *http://ptac.gov.lv/sites/default/files/01_tame_ptac_2018_01.pdf*.
23. Received written undertakings are published on the CRPC website at: *http://ptac.gov.lv/lv/table/rakstveida-apnemsanas*. Administrative decisions issued by CRPC are published on the CRPC website at: *http://ptac.gov.lv/lv/table/ptac-l-mumi*.
24. Available at: *www.em.gov.lv/en*.
25. Available at: *http://ptac.gov.lv/sites/default/files/gada-parskats-2018.pdf*.

26. Available at: *https://ec.europa.eu/info/live-work-travel-eu/consumers/enforcement-consumer-protection/sweeps_en*.
27. Available at: *www.ptac.gov.lv/lv/content/aizdomigo-interneta-vietnu-saraksts*.
28. Available at: *www.ptac.gov.lv/lv/content/k-izv-l-ties-dro-u-i-veikalu*.
29. More information is available at: *www.facebook.com/ptacgovlv/posts/1164183977095012*.
30. More information is available at: *www.facebook.com/ptacgovlv/photos/a.274069902773095/1111458369034240/?type=3&theater*.
31. Available at: *http://ptac.gov.lv/sites/default/files/docs/nr_19_vadlinijas_tiessaistes_speles_0.pdf*.
32. See more information at: *www.lia.lv*.
33. More information is available at: *https://likta.lv/en/home-en*.
34. See the Law On Out-Of-Court Consumer Dispute Resolution Bodies of 18 June 2015 at: *https://likumi.lv/ta/en/id/275063-law-on-out-of-court-consumer-dispute-resolution-bodies*.
35. Available at: *www.vvc.gov.lv/export/sites/default/docs/LRTA/MK_Noteikumi/Cab._Reg._No._631_-_Consumer_Claims.doc*.
36. Available at: *http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007R0861&qid=1408967394914&from=LV*.
37. Available at: *https://likumi.lv/ta/en/id/50500-civil-procedure-law*.
38. Available at: *www.em.gov.lv/en*.
39. Available at: *https://likumi.lv/ta/en/id/190612-rules-of-procedures-of-the-cabinet-of-ministers*.
40. See the Law On the Security of Information Technologies of 10 November 2010 at: *www.dvi.gov.lv/en/legal-acts/law-on-the-security-of-information-technologies*.
41. Available at: *https://cert.lv/en*.
42. Available at: *www.vp.gov.lv*.
43. Available at: *https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32004R2006*.
44. More information is available at: *www.ecclatvia.lv*.
45. Available at: *www.econsumer.gov*.

Chapter 6

SEIZING THE POTENTIAL OF THE DIGITAL TRANSFORMATION OF THE ECONOMY AND SOCIETY

Unleashing digital innovation

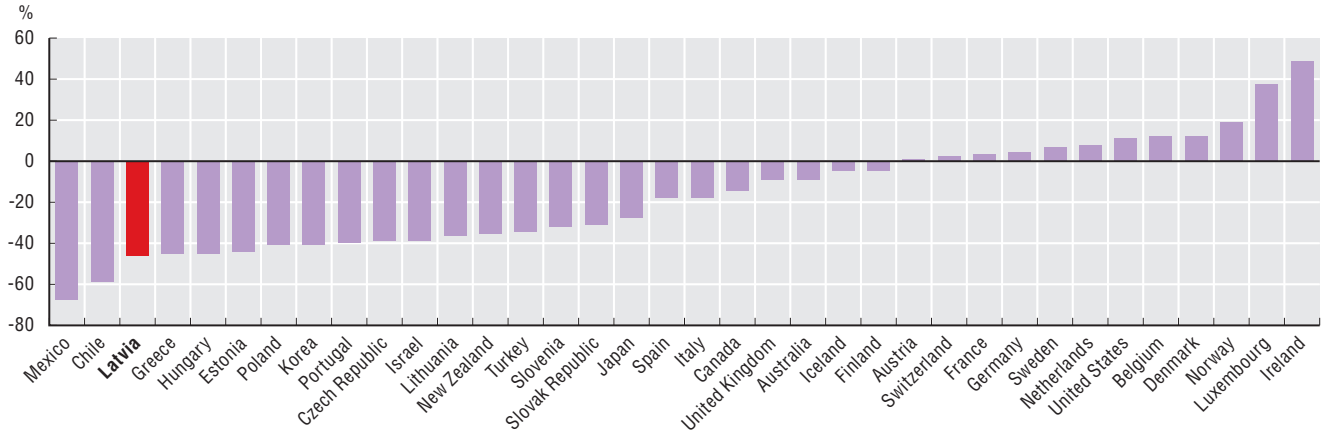
Latvia has made significant economic progress since the beginning of the millennium. The country's economy is growing faster rate than other EU and OECD countries. Productivity, however, remains significantly lower than in other OECD countries, while a declining working age population limits the prospects for further growth. Digital innovation is a key to increasing productivity and raising living standards. The Latvian government has thus taken measures to increase research and development (R&D) and innovation from its present low base. However, a more co-ordinated approach to implementing research and innovation policy, which treats ICTs as a transversal technology, could help Latvia raise its low innovation performance.

State of innovation and research in Latvia

Latvia is facing several challenges that may hinder future economic growth. The share of the working age population is shrinking due to an aging population and high emigration. In addition, while its small domestic market makes export-oriented growth a necessity, Latvia is distant from Europe's manufacturing hubs. Boosting innovation can help Latvia overcome these hurdles. Innovation can lift productivity from its current low level, thereby sustaining growth despite a falling population, and increasing wages, which can help to retain workers (Figure 6.1). In particular, digital innovation can overcome problems of distance and help Latvia boost exports.

Figure 6.1. Productivity gap in selected OECD countries, 2017

Percentage gap in GDP per hour worked against 17 richest OECD countries



Notes: Compared to the weighted average using population weights of the 17 OECD countries with highest GDP per capita in 2016 based on 2016 purchasing power parities (PPPs). Labour productivity is measured as GDP per hour worked.

Source: OECD (2019a), *OECD Economic Surveys: Latvia 2019*, *https://dx.doi.org/10.1787/f8c2f493-en*.

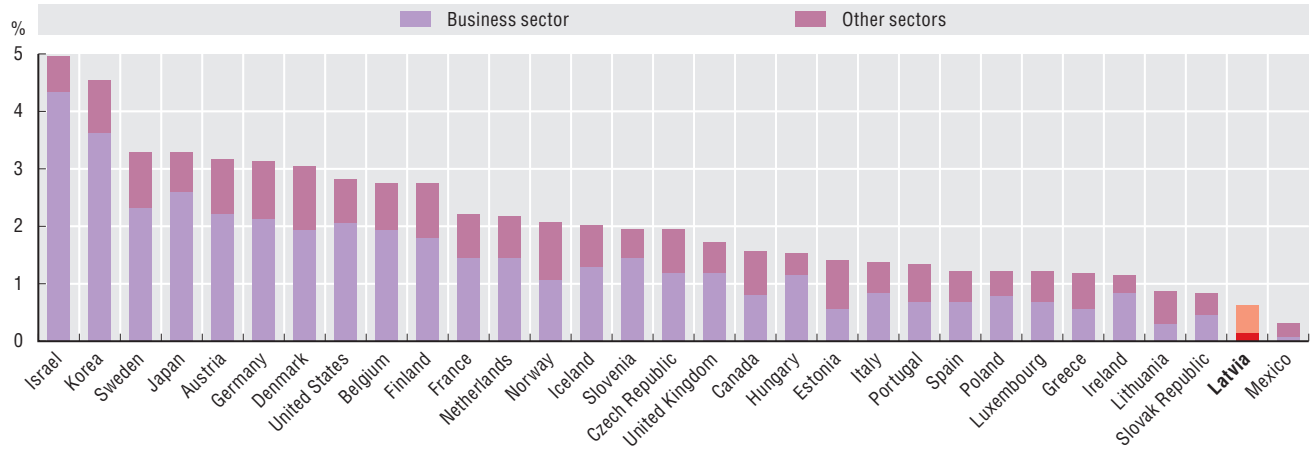
At present, innovation plays a relatively minor role in the Latvian economy. R&D is particularly low, even compared to countries with similar GDP per capita. Furthermore, almost a quarter of R&D is funded by the European Union (Figure 6.2). In addition, Latvia has among the lowest shares of business enterprise expenditure R&D in GDP in the OECD.

Latvia also performs poorly along other measures of innovation (European Commission, 2018a). The country has among the lowest shares of innovative small and medium-sized firms (SMEs) in the European Union (Figure 6.3). In addition, much of the innovation performed by Latvian firms focuses on the adoption of existing technologies, rather than developing frontier innovation leading to the creation of intellectual property. As a result, patent applications per inhabitant in Latvia are among the lowest in Europe (Lauma Muizniece, 2017) (Figure 6.4). Latvia's innovation gap is confirmed by its export specialisation in low-value added and resource intensive products (OECD, 2017a). In part, this poor performance can be explained by a large proportion of micro and small firms (see Chapter 4), which tend to be less innovative, and a stock of FDI below the EU average, with FDI diverted largely to sectors that tend not to invest in R&D (European Commission, 2018a; OECD, 2020a).

GOING DIGITAL IN LATVIA © OECD 2021

Figure 6.2. Business R&D expenditure in Latvia and selected OECD countries, 2018

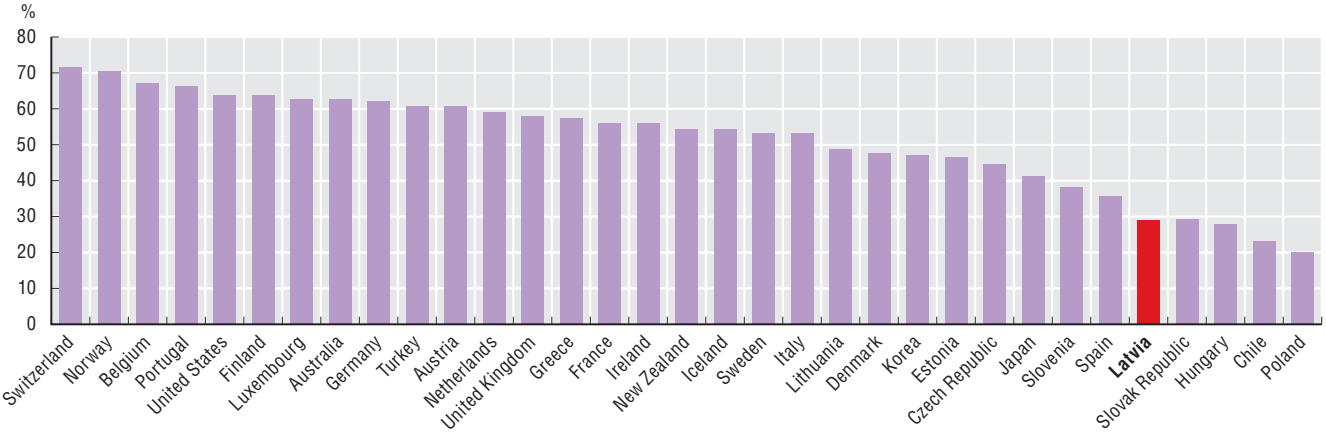
As a percentage of GDP



Source: OECD (2020b), *OECD Main Science and Technology Indicators* (database), *www.oecd.org/sti/msti.htm*.

Figure 6.3. Innovative SMEs[1] in Latvia and selected OECD countries, 2014-16

As a percentage of all SMEs

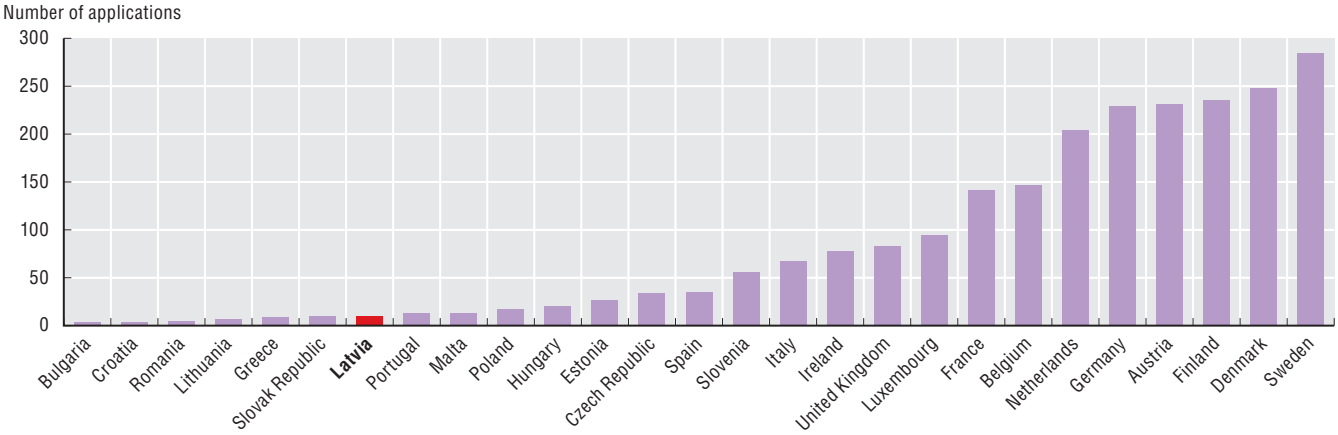


1. Innovative SMEs are those introducing product, process, marketing or organisational innovation.

Source: OECD, based on OECD (2019), *OECD Survey of National Innovation Statistics* and Eurostat, *Community Innovation Survey (CIS) 2016*, *http://oe.cd/inno-stats* (accessed on 20 January 2020).

Figure 6.4. Patent applications to the European Patent Office, 2017

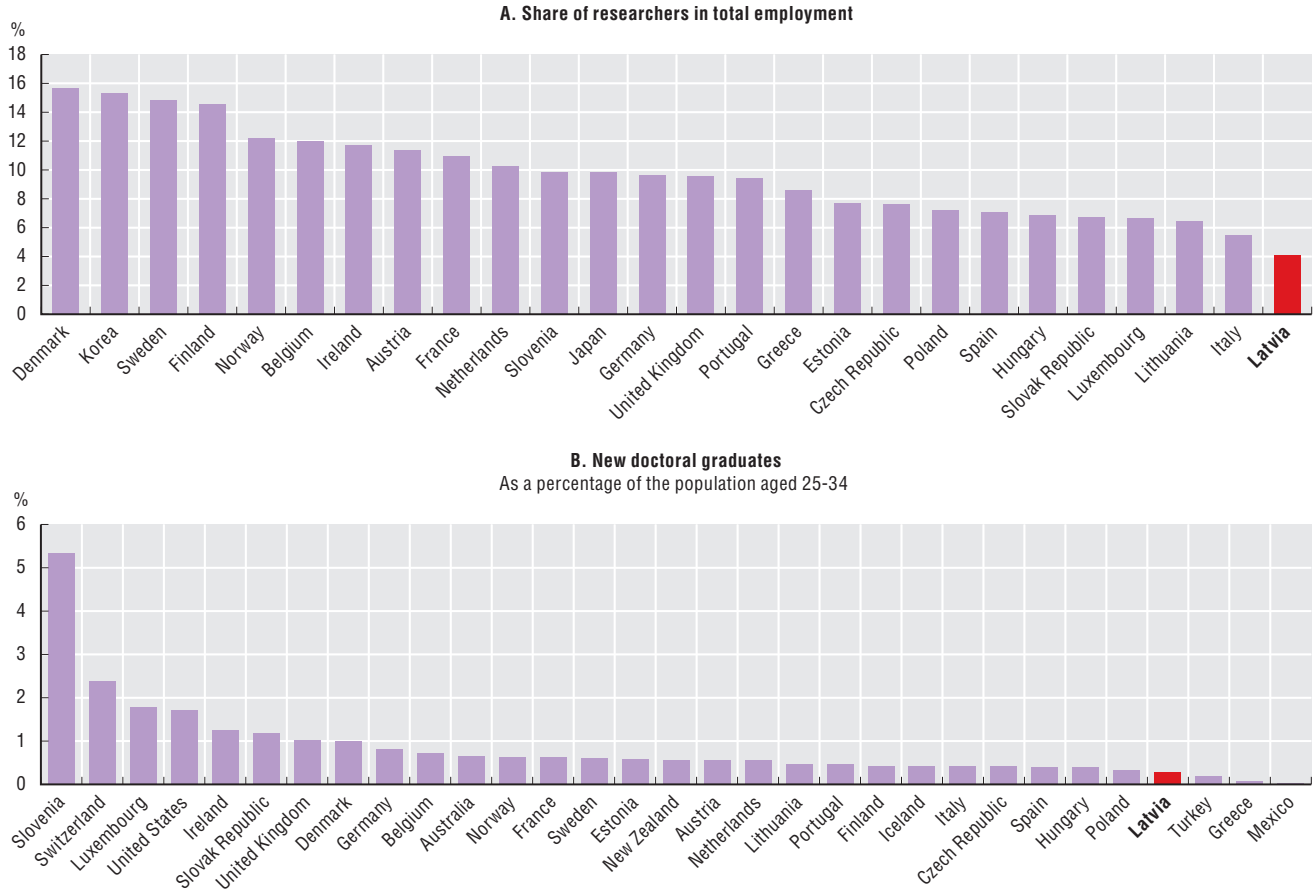
Per million inhabitants



Source: Eurostat (2020c), *Patent Applications to the EPO by Priority Year* (database), *https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=pat_ep_ntot&lang=en* (accessed on 6 May 2020).

The low innovation performance of firms is compounded by poor research performance in the higher education sector. Tertiary attainments for those aged 25-34 in Latvia are commensurate with the EU average, but the number of researchers and PhD graduates is particularly low (Figure 6.5) (OECD, 2019b). In addition, although the share of ICT specialists among all PhD graduates is in line with other European countries, it has shown some signs of decreasing in recent years (Figure 6.6) (Eurostat, 2019).

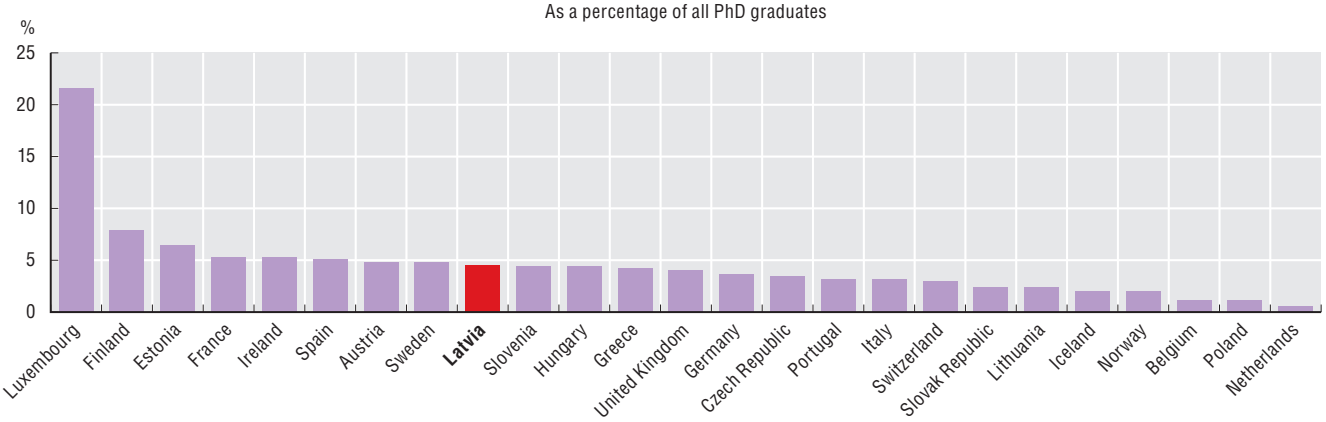
Figure 6.5. Researchers and new doctoral graduates in Latvia and selected OECD countries, 2018



Sources: OECD (2020b), *Main Science and Technology Indicators* (database), *www.oecd.org/sti/msti.htm*; OECD (2019c), *Education at a Glance*, *https://dx.doi.org/10.1787/f8d7880d-en*.

Figure 6.6. ICT PhD graduates in Latvia and selected OECD countries, 2013-17

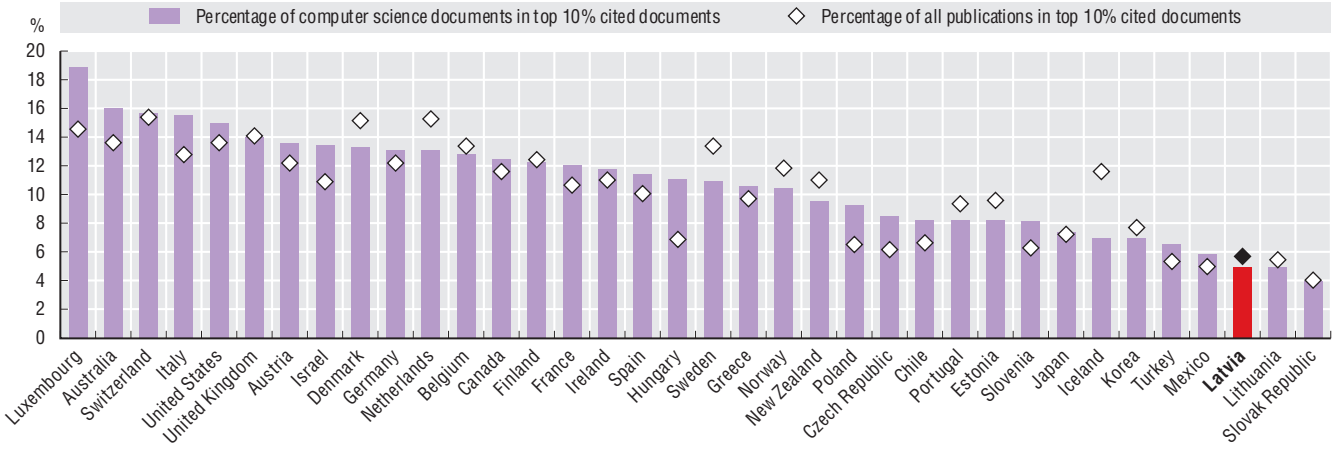
As a percentage of all PhD graduates



Source: Eurostat (2019), *Education Administrative Data from 2013 Onwards* (database), *https://ec.europa.eu/eurostat/cache/metadata/en/educ_uoe_enr_esms.htm*.

In addition, the quality of research is low relative to that of other EU countries (OECD, 2019a). Latvian publications in the field of ICT are under-represented in the top 10% most cited (Figure 6.7), and international collaboration is low (Figure 6.8).

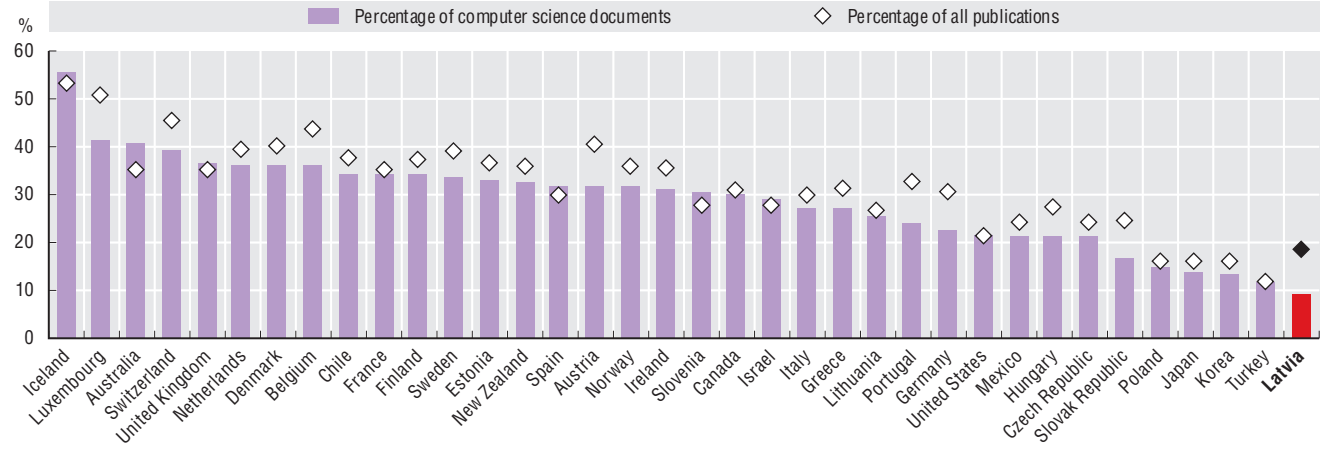
Figure 6.7. Top 10% most cited scientific publications in computer science in selected OECD countries, 2018



Note: Nationality is determined by the location of the institution to which the lead author is affiliated.

Source: OECD calculations based on Elsevier, Scopus Custom Data, Version 5.2019.

Figure 6.8. Scientific publications resulting from international collaboration in selected OECD countries, 2018



Note: Nationality is determined by the location of the institution to which the lead author is affiliated.

Source: OECD calculations based on Elsevier, Scopus Custom Data, Version 5.2019.

Innovation policy

Latvia's medium-term plans for innovation and entrepreneurship policy are set out in two sets of Guidelines: the *Guidelines for Science, Technology Development and Innovation for 2014-2020* (STDI) and the *Guidelines for National Industrial Policy 2014-2020*. These guidelines build on the long-term vision and direction put forward in the Latvia 2030 Strategy, which sets out medium-term objectives, defines the level of resources required and the tax initiatives to help achieve the objectives, as well as a set of indicators to monitor progress. Both Guidelines are consistent with the National Development Plan and the objectives of the Europe 2020 plan. Nevertheless, Latvia does not have a specific policy for the promotion of digital innovation, and the Guidelines do not single out ICTs as a key transversal technology for modernisation of the economy. In addition, digital technologies are not included as a key pillar of development in the draft National Development Plan 2021-2027 (Cross-Sectoral Coordination Centre, 2019).

The STDI Guidelines are based on Latvia's Smart Specialisation Strategy (also known as RIS3), which focuses on several high-value added sectors (see below) but lack provisions for the service sector (Box 6.1). Unlike previous guidelines, the R&D activities of firms and research institutions (e.g. universities) are now linked in a single planning framework. The Ministry of Education and Science (MoES), which sets policy for higher education and research, led the development of the Guidelines, with input from the Ministry of the Economy (MoE), various research institutes and the Latvian Information and Communication Technology Association (LIKTA) (Government of Latvia, 2013).

The STDI Guidelines and the Smart Specialisation Strategy acknowledge the ability of the ICT sector to help transform the Latvian economy. In addition, the development of a modern ICT system in the public and private sectors is listed as one of seven growth priorities. However, IT is not included as a stand-alone priority direction for science (Cross-sectoral Coordination Centre, 2017).

Box 6.1. Implementing the Guidelines for Science, Technology Development and Innovation

There are four lines of action for implementing the STDI Guidelines. These have specific associated tasks, such as tax measures or the introduction of innovation vouchers, as shown below.

- Increasing the competitiveness of the STI field:
  - Develop the human resource capital of the field.
  - Develop excellence in research.
  - Reduce STDI resource fragmentation.
  - Support the internationalisation of science and international co-operation.
- Linking science, technology and innovation with the needs of social and economic development:
  - Build the knowledge base and focus research on directions important for society's development.
  - Promote orders from industry ministries and municipalities.
  - Integrate education, the development of science, technology, innovation and business.
  - Strengthen innovation and knowledge absorption capacity in companies.
- Ensuring effective management of the STI industry:
  - Improving co-ordination.
  - Increase investment efficiency.
  - Increase state budget funding for STDI.
  - Calculate and allocate institutional or base funding in accordance with policy settings.
  - Gradually increase the level of R&D funding granted in tender procedures.
  - Create new financial instruments appropriate for the aims and tasks of STDI policy.
  - Support research in higher education (HE investments).
  - Develop a policy implementation, monitoring and impact assessment system.
- Raising public awareness and promoting science and innovation

The MoE has developed the *Guidelines for National Industrial Policy 2014–2020* (NIP). This set of guidelines relates largely to the manufacturing sector and recalls the EU target of raising Latvia's R&D expenditure to 1.5% of GDP – a target that is very unlikely to be met. They underline the importance of improving co-operation in innovation between research institutions and firms (European Commission, 2012a), but make no reference to digital technologies (unlike Sweden) (Box 6.2), despite discussing the importance of modernising the Latvian economy.

In addition, relatively little focus is placed on the development of digital services or service innovation, in spite of the strong link between digital innovation and the delivery of digital services. New business models have emerged, such as peer-to-peer accommodation (as with Airbnb), and new web-based

business services have become a possibility. In addition, digitalisation blurs the line between goods and services, for example when sensors are incorporated into manufactured goods which can then be monitored as a service. (OECD, 2019d).

Box 6.2. Sweden's Innovation Strategy

Sweden's innovation strategy for 2017-2020 is set out in its research bill "Knowledge in collaboration – for society's challenges and strengthened competitiveness" (*Kunskap i samverkan – för samhällets utmaningar och stärkt konkurrenskraft*). The bill was elaborated to ensure Sweden becomes a world leader in research and innovation (OECD, 2018c; Swedish Ministry of Education and Research, 2019).

This strategy highlights the importance of Sweden's large ICT sector and ability of digital technologies to function as an enabler of innovation in other fields. The strategy includes:

- investment in digital research infrastructure (e.g. the Swedish University Computer Network) to facilitate data intensive research
- grants for data-driven research
- the promotion of open access to research data, such as through the use of personal identity numbers to connect different public registers and facilitate medical and social science research.

Latvia should undertake action to promote digital services, following the examples of several other OECD countries. In Austria, for instance, the Smart and Digital Services Initiative provides funding for non-technological innovations with the aim of promoting R&D in the service sector and encouraging firms in traditional industries to provide services (e.g. by including sensors in products and providing monitoring services as part of Industry 4.0). Small firms can avail themselves of non-repayable subsidies of up to 45% (FFG, 2015; OECD, 2020c). Meanwhile the Netherlands Enterprise Agency offers service design vouchers worth up to EUR 3 000 to SMEs in the manufacturing sector on condition that they also invest at least EUR 1 000. The vouchers can be used for consultancy advice with the intention of boosting co-operation between creative industries and manufacturing (OECD, 2019d; RVO, 2018).

Latvia's innovation strategy also lacks an emphasis on developing apps and software to address some of the country's societal and economic challenges. For example, Colombia's 2014-2018 Live Digital for the People (*Vive Digital para la Gente*) plan included the aim of making Colombia a world leader in developing apps to help the poorest in society. This goal helped the development of an agricultural app (Farmapp) to help pest control, which has been exported (OECD, 2019e). Meanwhile the United Kingdom has created the Centre for Acceleration of Social Technology, which has helped charities develop apps to meet their goals.

Promotion of R&D

Most of Latvia's government research funding goes to HEIs – and almost none to businesses (European Commission, 2018a) (Figure 6.9). Although Latvia used to provide a generous R&D tax allowance, this was abolished in 2018 as part of the reform of corporate income tax whereby only distributed income is taxed (e.g. payment of dividends). The majority of support for business R&D now takes the form of direct funding and tax incentives for hiring R&D staff (see below), in contrast to most OECD countries (Box 6.3) (OECD, 2019q; 2018a).

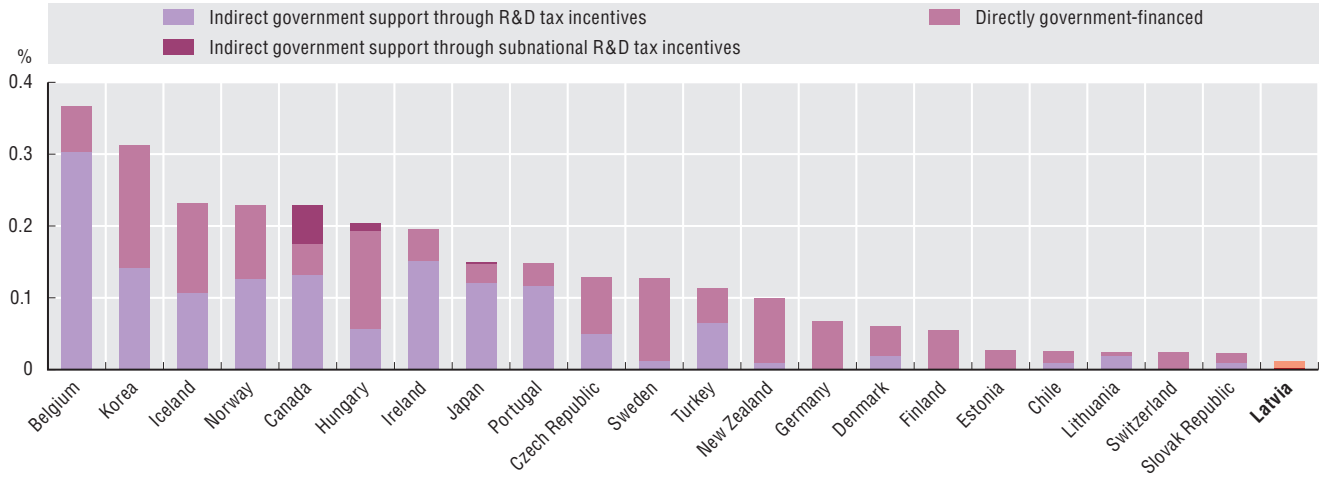
HEIs receive low levels of research funding

The Latvian HEI sector suffers from low levels and wide dispersion of funding. Public research funding amounts to EUR 73 million, half of which comes from the European Union; little of this funding is awarded competitively, with the majority allocated to finance the basic functions of institutions (see below) (European Commission, 2018a; OECD, 2019a). In addition, financial resources for research are thinly spread, with 21 public sector research institutions (including those based in universities) and scientific institutions receiving state and ERDF funding (European Commission, 2018a). Latvia also has more HEIs than Estonia or Lithuania; however, the University of Latvia (UL) and Riga Technical

University (RTU) account for over 40% of researchers and academic staff in the HEI sector (European Commission, 2018a). Latvia should therefore continue to concentrate research funding in a smaller number of institutions to allow the formation of institutions with a deeper pool of expertise.

Figure 6.9. Government funding and tax support for business R&D in Latvia and selected OECD countries, 2017

As a percentage of GDP



Note: R&D = research and development.

Source: OECD (2019f), *R&D Tax Incentives* (database), *www.oecd.org/sti/rd-tax-stats.htm*.

Box 6.3. Various approaches used to promote R&D

Governments can help support R&D directly (e.g. by providing grants or buying R&D services) or indirectly through fiscal incentives such as through preferential tax treatment of R&D expenditures or income. In the OECD area, almost 70% of all support for R&D is through indirect measures (Appelt et al., 2016).

A benefit of direct supports is that they can be targeted at areas that offer the highest social returns, but the administration of grants and the selection of projects can be costly. Direct support is considered most appropriate for research that will lead to public goods, and for riskier activities, such as helping firms to scale up. Market-based measures such as tax incentives have the advantage of not being dependent on the discretionary decisions of government officials, making them easier to administer and more likely to be compliant with international trade rules. Tax incentives are useful to stimulate an increase in R&D, especially in firms where R&D is already performed. However, they are not effective at directing research towards areas with higher social returns, and are more appropriate for the promotion of research that will lead to commercialisation. Loans are appropriate for diffusion-oriented R&D where there is also a need for capital expenditure.

Tax incentives can be calculated based either on expenditure on R&D or the income derived from R&D. Expenditure-based incentives include tax allowances, exemptions and deductions, which reduce the size of the tax base. In general, these rely on the firm having a sufficiently large tax liability (although tax credits can be refundable). An alternative approach (which is used in Latvia) is to reduce other R&D costs such as payroll taxes for research staff. These act as an upfront subsidy and are more attractive to riskier research, conducted in some cases by young firms, which are more likely to be loss-making or financially constrained. Finally, an alternative approach is to give preferential treatment to income from R&D (e.g. patent royalties). However, it can be more difficult to link income to R&D activities (Appelt et al., 2016; OECD, 2019q).

The lack of funding is compounded by the absence of an effective career structure for researchers, which can inhibit retention of skilled researchers and the development of research capacity. In addition, many university researchers are near retirement (European Commission, 2018a). Hiring is made more difficult by Latvian language requirements, as public universities must offer courses in Latvian, and academics must be fluent in Latvian (although an exception is made for visiting academics with a contract of less than two years) (The World Bank, 2018b). In addition, the government is setting up a database of Latvian researchers abroad to try to overcome hiring difficulties and encourage research and teaching collaboration (OECD, 2019a).

Latvia is also introducing new hiring criteria for professors, who will need a minimum number of academic publications, in order to increase the number of active researchers in HEIs (European Commission, 2018a). However, HEIs do not offer tenure, with contracts lasting for six years, which can make it difficult to attract talented researchers (OECD, 2016). The Latvian government is planning to ease the hiring of staff by merging career structures for research staff and academic staff. In order to encourage applied research and innovation (e.g. developing prototyping and patenting), the ability of researchers to attract external funding should be included as a criteria for promotion.

Funding of HEIs has been reformed to boost research orientation

To increase the emphasis on research in HEIs, the government has introduced a new funding model (European Commission, 2018a). There are now three pillars of funding in HEIs: basic funding, which depends on the average cost of teaching per student; performance-related funding, which is linked to the number of researchers who graduated no more than five years ago, the amount of international research funding attracted, the amount of funding attracted via R&D contracts, the amount of funding attracted from local governments, and the amount of funding attracted from creative and artistic projects; and innovation-oriented funding, which comes almost entirely from EU innovation projects (see below) (The World Bank, 2018a). In 2015, 60% of funding went to basic funding, 20% to performance-related funding and 20% to innovation-oriented funding (OECD, 2019g). However, in 2018, 90% of funding went to cover basic activities, with only 2% allocated to innovation-oriented activities.

Research funding is science focused rather than market-oriented

Latvia largely supports research through grants, and has two systems for administering funds for research and innovation depending on whether the source is the Latvian government or the European Regional Development Fund (ERDF). In 2017, each source accounted for an approximately equal amount of funding. National programmes tend to be smaller in scale but run over a longer period, while the opposite is true for structural funds programmes (i.e. they are bigger but run over a shorter time span) (European Commission, 2018a).

Latvian government research funding is administered by the MoES and its agencies (with the exception of research programmes of the Ministry of Agriculture), with the MoES also designing national funding programmes. The State Education and Development Agency (SEDA) administers funding from international sources such as ERDF-co-funded post-doctoral research programmes, international R&D co-operation programmes, and programmes funded by the European Economic Area and Norway. Meanwhile the Studies and Research Administration (SRA) administers fundamental and applied research programmes, student loans and research programmes that fall under the competence of the MoES. The Latvian Council of Sciences organises international peer review for state funded programmes (European Commission, 2018a). In addition, the Latvian Academy of Sciences provides small grants to senior scientists of repute.

EU-funded R&D and innovation programmes, including projects to modernise research infrastructure, are administered by the Central Finance and Contracting Agency (CFCA), which administrates all EUR 4.4 billion in EU funds made available to Latvia for the period 2014-2020 and is answerable to the Ministry of Finance (MoF). The CFCA has increased in importance since 2014, when it became the only co-operation institution for EU cohesion funds. The CFCA selects projects and administers them financially and scientifically (CFCA, 2020). As with SEDA, the CFCA selects peers from the European Commission's database for Horizon 2020 or other equivalent databases of international scientific peers. However, the role of the CFCA does not extend to supporting project leaders in the implementation

of their projects (as is typically done by innovation agencies such as the Latvian Investment and Development Agency) (CFCA, 2019; European Commission, 2018a).

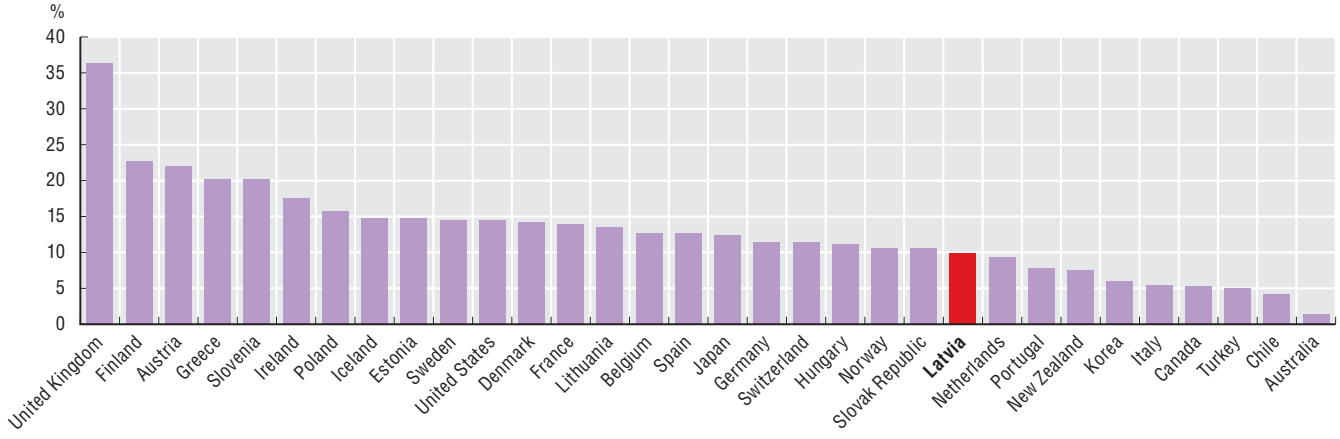
A benefit of the CFCA is the creation of a one-stop shop for applying for EU funds. However, the dual system results in implementation agencies answering to the MoF rather than to line ministries responsible for their policy. It also leads to agencies competing with CFCA reviewers of projects. From July 2020 onwards, a new Latvian Science Council will take over all the functions of implementing science policy from the current Latvian Science Council, SEDA and the SRA (MoES, 2020a). This should help improve programme efficiency in support of innovation.

Incentives to collaborate with firms are weak and ICT projects receive a small proportion of funding

Incentives for HEIs to collaborate with industry have been weak, however, with only a few SMEs collaborating with research institutions (European Commission, 2018a) (Figure 6.10). The new performance-related funding pillar for HEIs has changed these incentives, giving more funding to HEIs that collaborate with firms (OECD, 2019a). In addition, ERDF-funded applied research programmes, the Competence Centres programme and the Technology Transfer Programme (below) have served to boost links. Further increasing the proportion of HEI funding that depends on collaboration with firms could help to increase the market orientation of research conducted in HEIs.

Figure 6.10. SMEs co-operating on innovation activities with higher education or government institutions in selected OECD countries, 2014-16

As a percentage of innovative enterprises[1]



1. Innovative SMEs are those introducing product, process, marketing or organisational innovation.

Source: OECD, based on OECD (2019), *OECD Survey of National Innovation Statistics* and Eurostat (2016), *Community Innovation Survey (CIS) 2016*, *http://oe.cd/inno-stats* (accessed on 20 January 2020).

In addition, only a small proportion of EU research funding goes towards ICT-related projects in Latvia. The applied research ERDF funding stream, administered by the CFCA, aims to boost the research capacity of Latvian institutions. However, out of the 74 research projects running at the end of 2019, only two were in the field of ICT, with funding of EUR 750 000 (i.e. 1.9% of the total programme funding) (EsFondi.lv, 2020a; 2020b). The Postdoctoral Research programme, administered by SEDA, had 194 projects running at the end of 2019 (with almost EUR 25 million), out of which only one was in the field of ICT, with funding of approximately EUR 100 000 (i.e. 0.4% of total programme funding). Allocating a greater proportion of research funding to ICT-related projects should be a priority for Latvia to foster innovation capacity in this sector.

More funding should be awarded competitively and based on broad impact criteria

Latvia should raise the quality of research by increasing the proportion of funding awarded competitively. Competitive funding of projects can ensure projects reach a minimum level of quality, and gives researchers an opportunity to test ideas among peers, although there is mixed evidence that this

can lead to shorter-term low-risk projects being selected, while increasing the administrative burden on researchers and hindering long-term planning. There is wide variation across OECD countries for the proportion of research funding awarded competitively, typically ranging from 25% to 50% (OECD, 2018b). Nevertheless, Latvia should increase the proportion of research funding allocated through a competitive process. Setting aside a proportion of more junior researchers would help overcome difficulties in attracting funding due to lack of a track record.

Latvia largely offers funding *ex ante* rather than rewarding successful research and innovation *ex post* (OECD, 2019g). If CFCA-funded projects have a negative *ex post* evaluation expenses must be refunded, though this has not occurred to date (MoF, 2020). Part of research funding should be based on the impact of research. For example, Science Foundation Ireland has gone beyond the use of bibliometric citations and introduced research impact evaluations, whereby experts in the commercialisation and development of research evaluate the impact of research *ex post*. In addition, for many projects international experts conduct a mid-term review to assess progress against the original proposal (OECD, 2018b).

Promotion of innovation within firms

Innovation does not play a large role in Latvian firms (see above). However, Latvia is taking steps to increase the number of firms involved in innovation through regional and ERDF-funded programmes. Nevertheless, lack of clarity about the role of ICTs in national planning documents has led to programmes with overlapping and, at times, inconsistent aims.

The Latvian Investment and Development Agency (LIDA) plays an important role in managing support programmes for entrepreneurs. The LIDA is the main state agency for innovation and forms part of the MoE. It manages innovation programmes funded by EU structural funds such as the Technology Transfer Programme, the Innovation Motivation Programme and the Business Incubators Programme (although the CFCA administers funding). The LIDA's main role is to support foreign direct investment (FDI), although FDI flows largely towards sectors that do not tend to invest in R&D (European Commission, 2018a).

Latvia has sought to increase public awareness of the benefits of innovation and has taken measures to encourage those with innovative ideas to pursue them to commercialisation. For instance, the Innovation Motivational Programme aims to raise awareness among the general public of the importance of innovation and to encourage entrepreneurship. The programme receives ERDF funding (EUR 0.5 million in 2018) but is run by the MoE and LIDA. Activities to date have included a "brainstorming" competition to generate business ideas, networking events, management innovation training for merchants (e.g. a week-long Mini-MBA in Innovation and Leadership course) and competitions such as the Ideas Cup for innovative business ideas (Cross-sectoral Coordination Centre, 2017; LIDA, 2019a).

There are overlapping programmes to link firms with HEIs and research institutes

Several programmes exists to boost innovation by diffusing expertise across Latvian firms. However, these programmes do not regard digital technologies as key enablers of innovation. Introducing a strong digital focus in these programmes is crucial for Latvian firms to seize the innovation opportunities arising from the digital transformation.

In 2010, Latvia launched the Competence Centre Programme, managed by the LIDA, to raise the competitiveness and innovation of firms. These centres aim to promote applied research and frontier innovation in sectors aligned with the Smart Specialisation Strategy (see below) and, thereby, help develop new products and technologies by fostering co-operation between the research sector and industry. However, in this regard the centres overlap with the Technology Transfer Programme (above). Although the competence centres receive grant funding from the ERDF, they are majority owned by the private sector, and at least a quarter of their funding must be earmarked for experimental development. By the end of 2018, support was given to almost 150 firms to create or improve 174 products, with almost 500 jobs created, 175 master and doctoral students involved in research, and over 200 academic articles published.

The IT Competence Centre began operating in April 2011 and focuses on the areas of natural language technologies and business process analysis technologies, with previously conducted studies leading to publication in academic journals. The centre received EUR 7.8 million in ERDF funding plus private funding of EUR 5.2 million for the period 2014-20. Over the period April 2019 to December 2021, 20 research projects are being implemented with the intention of assisting 20 firms to develop new products (Esfondi.lv, 2020c). Given that ERDF funding is due to expire in 2021, alternative sources will be required. Increasing the proportion of funding from private co-financing could help ensure that incentives are geared towards generating commercial innovations, rather than academic research.

In contrast, the Technology Transfer Programme aims to boost innovation in SMEs by diffusing existing technology and expertise (rather than engaging in frontier innovation) from research institutions and promoting the commercialisation of research. The programme is administered by the LIDA but receives funding from the ERDF. Entrepreneurs are directed towards potential research organisations by "technology scouts" who work for the LIDA.

The Technology Transfer Programme mainly offers support to established SMEs in the form of innovation vouchers, although it also helps to finance visits with potential investors and participation in trade fairs for start-ups, and assists research institutes with commercialising their research. Innovation vouchers are available for any business that develops new products or technology in sectors outlined in the Smart Specialisation Strategy. Vouchers are co-financed 85% up to the value of EUR 25 000 and can be used for feasibility studies, experimental development, prototyping, industrial design, strengthening intellectual property, and for testing and certification (LIDA, 2019b; 2019c). Support of up to EUR 300 000 is also available to research organisations for feasibility studies and for developing commercialisation strategies. By the end of 2018, the programme had spent EUR 2.7 million and 36 new products or technologies had been developed, 48 firms had received grants to launch new products on the market (e.g. by visiting potential investors and exhibitions), and 15 projects of research organisations had financed for commercialisation. The project will continue to the end of 2022 (Esfondi.lv, 2020d).

Latvia has sought to foster innovation by boosting co-operation among firms

Technology diffusion can also be boosted by increasing co-operation among innovating firms and multinational enterprises (MNEs), an approach that has been lacking in Latvia (OECD, 2017a). The Cluster Programme aims to increase the competitiveness export capacity of SMEs by increasing co-operation among firms within the same sector. The programme supports 14 clusters, as defined by the Smart Specialisation Programme (MoE, 2018a). The Latvian IT Cluster includes both firms and HEIs as members, and provides services to assist in exporting, for example by providing firms with information about international networking events and market research. However, these activities overlap with the export promotion work of the LIDA. In addition, the IT Cluster organises events to promote digitalisation in other sectors, ranging from workshops for individual firms to highlight the benefits of digitalisation to larger networking events. These activities appear to duplicate those of the ICT sector association LIKTA.

The Latvian IT Cluster is also one of three Digital Innovation Hubs (DIHs) in operation, with a fourth being established in Riga. The aim of these hubs is to boost cross-sectoral collaboration. The second DIH, the Ventspils High Technology Park (VHTP) (based in Ventspils, almost 200 km from Riga), focuses on developing hardware such as smart materials, technology and engineering within the manufacturing sector, and offers services to assist firms in their digitalisation efforts. The third, the Institute of Electronics and Computer Science (EDI), is a state research institute originally established in 1960 that develops software (e.g. signal and image processing) and embedded hardware (e.g. remote sensors and wearable devices) (European Commission, 2018b). An additional DIH, TechHub Riga, will be based in Riga. However, the proliferation of various hubs can potentially limit the development of a critical mass of expertise. Latvia should therefore consider instead concentrating funding within fewer organisations.

The presence of the Latvian IT Cluster in both the Cluster Programme and the DIHs can lead to conflicting aims, creating a critical mass of expertise, on the one hand, and diffusing such expertise, on the other. Given the overlap between the IT Cluster, LIKTA, LIDA and the IT Competence Centre, the Latvian government should review the activities of these organisations, assess their relative strengths and weakness, and clearly define their respective roles based on this assessment. In addition, these programmes should focus on promoting digitalisation within firms, rather than innovation within the IT sector.

To some extent, this duplication among programmes is an outcome of the *Guidelines for National Industrial Policy*, which do not recognise digital technologies as a key transversal enabler of innovation, and make no distinction between the adoption of existing technologies and the promotion of frontier innovation. Placing digital innovation at the core of the *Guidelines for Science, Technology Development and Innovation* and the *Guidelines for National Industrial Policy* will allow Latvia to set clear priorities for its programmes, reduce overlap and increase efficiency.

Adapting intellectual property and regulatory regimes could boost digital innovation

Measures have also been taken to improve the protection of intellectual property rights (IPRs), which can help develop frontier innovation. Latvian IPRs policy is fragmented across the Ministry of Justice (MoJ), the Ministry of Culture (MoC) and the Ministry of Agriculture (MoA), with different agencies responsible for copyright, patents and trademarks (Cross-sectoral Coordination Centre, 2017). This can be particularly problematic for digital innovation, which frequently spans several IPRs mechanisms (Beckerman-Rodau, 2011). Latvia has improved the situation by establishing an Intellectual Property Council as an advisory body and a single Intellectual Property Information Centre to provide information and consulting services regarding the different forms of intellectual property (Patent Office of the Republic of Latvia, 2019). Meanwhile, Latvia's Patent Office (LRPV) offers search reports, which can help reduce costs for those applying for a European patent. In addition, the LRPV and the LIDA are increasing awareness among firms of the importance of IPRs through events such as seminars and trade fairs. Modules on IPRs will also be incorporated into tertiary courses on graphic design and technical subjects.

Developing an Intellectual Property Strategy, as has been done in some Nordic countries, could help Latvia increase investment in IPRs. For example, Finland published its first IPRs strategy in 2009 (currently under review) to overcome problems such as lack of knowledge among SMEs regarding potential IPRs, lack of ability to establish contracts capitalising on their IPRs and an inability to monitor whether their IPRs are being violated (OECD, 2011). This strategy included steps to improve the efficiency of IPRs protection in the court system through the establishment of a dedicated court and tax incentives for R&D (Takalo, 2013).

Finally, navigating regulations can be a challenge for new digital firms (see below). In response, Denmark has created a one-stop shop (Nye Forretningsmodeller) for regulatory inquiries about new business models, which may be impacted by new regulations administered by different public authorities. This agency also analyses the demands of new businesses and the ways in which regulations are implemented in neighbouring countries, in order to develop new solutions to regulatory challenges (Nye Forretningsmodeller, 2019).

Promotion of start-ups

Latvia has also expanded its efforts to support start-ups along all stages of their life cycle. Latvia has 400 registered start-ups, which are mostly concentrated in Riga, although the city has been described as a start-up community rather than a start-up ecosystem (European Commission, 2018a; LIDA, 2019d). In 2018, StartupLatvia.eu was launched as a portal listing the services offered to start-ups. In addition, creating a favourable environment for innovation and start-ups was made a central tenet of Latvia's innovation policy. The MoE is also implementing an Action Plan for Enhancing the Environment for Entrepreneurship (OECD, 2019g). In recent years, Latvia has taken further measures, such as easing access to finance and reforming tax laws, which can be of particular benefit to digitally innovative firms (see below).

The Business Incubator Programme, which runs from 2016 to 2023, offers training and mentoring for later stages of the innovation process (OECD, 2019h). Incubators are located across Latvia, with a Creative Industries Incubator in Riga (LIDA, 2019e). In total, there are 15 incubators across Latvia (with two in Riga) run by the LIDA, which offer training, mentorships and grants for a maximum of four years. The incubators offer training in the use of digital tools, and some of the incubated firms now sell digital products (e.g. VRDEV developed virtual and augmented reality). However, the aim of these incubators is to foster entrepreneurship across Latvia rather than developing digital technologies (LIDA, 2019f). Latvia should therefore reorient the efforts of one of its hub towards digital start-ups.

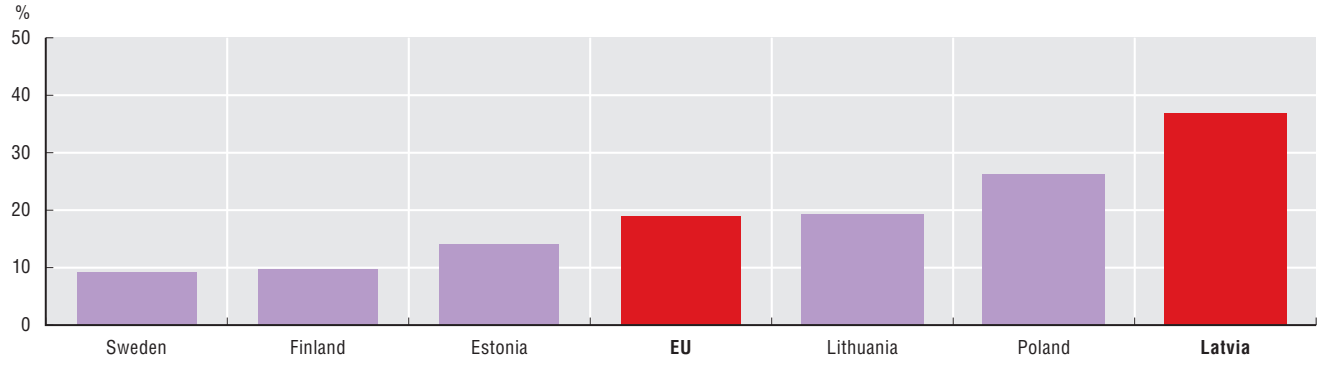
Finally, in 2019 the MoES approved five HEIs to provide grants to students as part of the ERDF-funded Innovation grants for students programme. This programme aims to develop the entrepreneurship and innovation skills of students through training in product development, commercialisation and the establishment of business incubators for students (EsFondi.lv, 2020e; RTU, 2019). Total funding of EUR 14.25 million was approved, with a quarter coming from the private sector.

Measures have recently been taken to ease access to finance

Firms face obstacles accessing finance which can act as a barrier to innovation. Almost half of firms report financing as an obstacle to investment (Figure 6.11). SME lending has remained low since the financial crisis, with smaller firms getting most of their funding from equity and non-bank short-term liabilities such as trade credit (OECD, 2019h). This has led the government to take measures to increase financing.

Figure 6.11. Firms declaring that availability of finance is a major obstacle to long-term investment, 2018

As a percentage of all firms



Source: European Investment Bank, *EIB Investment Survey 2019*.

ALTUM is Latvia's sole development finance agency. It was created in 2013 out of the merger of the Latvian Guarantee Agency, Lavijas Hipotēku un Zemes Banka and the Rural Development Fund (OECD, 2019i). It is owned by the ministries of Agriculture, Economics and Finance (European Commission, 2018a). ALTUM implements state aid programmes, such as microfinance, credit guarantees and loans to start-ups, some of which are funded by the European Union (Cross-sectoral Coordination Centre, 2017; OECD, 2019a). The agency initiated micro-loans in 2016 for start-ups followed by loan guarantees in 2017 (OECD, 2019h).

Four acceleration funds operate in Latvia, all of which have demonstrated considerable attention to digital innovation. In 2018, 15 million EUR (with funding provided by the ERDF but administered by ALTUM) was provided to three acceleration funds, two of which fund the development of digital technologies. Overkill Ventures focuses on business-to-business software start-ups and BuildIT focuses on hardware and the Internet of Things (LIDA, 2019d). In 2019, the first 18 start-ups advanced past the accelerator stage (ALTUM, 2019).

In addition, seven new venture capital funds (backed by the European Union) were launched in 2018 (OECD, 2019h). Venture capital funds have expanded due to an increase in public funding, though the venture capital market remains small due to a lack of good investment opportunities (OECD, 2019a). The Baltic Innovation Fund (BIF) is part of the European Innovation Fund (EIF) and combines funding from the three Baltic governments (OECD, 2019g).

Improving the environment for start-ups

Latvia has also taken measures to ease migration for those working for or who have founded start-ups, and also to protect IPRs.

In May 2017, a special visa programme for those launching start-ups was introduced. Latvia offers temporary residence permits (referred to as the "start-up visa") for up to three years to non-EU start-up founders that base themselves in Latvia. Each start-up can have up to five founders availing themselves

of a residence permit. Permit holders are not allowed to be an employee or board member of another company in Latvia and must attract an investment of at least EUR 30 000 from a venture capital fund or 15 000 from an accelerator or business angel within 12 months (LIDA, 2019g).

In 2017, a Start-up law also came into effect, offering eligible firms two options for reducing the cost of hiring highly skilled R&D staff, including ICT specialists. The first option allows firms to pay a lump-sum social insurance contribution of EUR 302 per month for each employee regardless of the salary paid as an alternative to the overall 35% social security rate. This option is more convenient for firms where staff are paid at least double the minimum wage. In addition, start-up employees are exempted from personal income tax on their salary. Alternatively, firms can opt for a 45% rebate on the labour cost of highly qualified staff who hold a MSc or PhD degree (in information technology, natural sciences, mathematics, engineering and technology, manufacturing and processing, or design) or at least three-year's work experience in a relevant field. Eligible firms can receive these benefits for one year initially and can continue for a maximum of five years (Magnetic Latvia, 2019).

Total funding for assistance under the Start-up law has been capped at EUR 1.6 million and is available via ERDF and national sources (LIDA project No. 1.2.1.2/16/I/001) (LIDA, 2019d). Nevertheless, it is unclear whether it is more beneficial for Latvia's scarce ICT specialists to work in start-ups rather than in more established firm. In addition, Latvia lacks other market-based incentives to promote R&D. Latvia should therefore consider making the tax incentives for R&D staff in start-ups less generous but available to all firms.

Conclusion and policy recommendations

There is considerable overlap among Latvia's efforts to boost innovation. In part, duplication is a result of digital technologies not being included as a transversal enabler of innovation across several sectors. The duplication of efforts among the LIDA, competence centres, clusters and hubs can hinder the development of institutional expertise within a single organisation. In addition, projects have seemingly been chosen because of their ability to attract EU funding, rather than based on a clear set of national priorities. As EU programmes tend to be short term in length, this further hinders the development of institutional capacity to support innovative firms. Therefore, creating a new innovation strategy, with digitalisation at its heart can help Latvia reduce such duplication. Key recommendations are presented in Box 6.4.

Box 6.4. Policy recommendations

Boosting research

- Review the *Guidelines for Science, Technology Development and Innovation* and the *Guidelines for National Industrial Policy* for the next planning period and:
  - put a strong focus on digitalisation as a key transversal enabler of innovation and growth
  - promote digital service innovation
  - promote digital innovation to address Latvia's societal and economic challenges.
- Increase the level of public support to business R&D and diversify its composition towards greater use of tax allowance for R&D expenditures.
- Increase incentives for HEI staff to engage in applied research and innovation, by incorporating their ability to raise private funding among the criteria for promotion.
- Allocate a greater proportion of research funding to ICT-related projects (including cross-disciplinary projects), which are currently underfunded.
- Raise the quality of research by increasing the proportion of funding allocated through competitive processes.
- Introduce a system of *ex post* evaluation of research projects similar to that used by the Science Foundation Ireland.

Box 6.4. Policy recommendations *(cont.)*

Boosting innovation in firms

- Raise the proportion of private co-financing of competence centres to ensure that they are geared towards commercial innovations.
- Review the activities of the IT Cluster, LIKTA, LIDA and the IT Competence Centre to assess their relative strengths and weakness, and clearly define their respective roles based on this assessment.
- Clearly focus the mission of the IT Cluster on promoting digitalisation among firms to avoid duplication with other programmes.
- Develop an intellectual property rights (IPRs) strategy, based on the successful example of Finland, and establish a specialised court for all IPR issues.
- Raise business incentives to invest in R&D by making existing tax incentives for R&D staff in start-ups less generous but available to all firms.

Latvia's Smart Specialisation Strategy

In 2013, the Latvian government adopted a National Research and Innovation Strategy for Smart Specialisation (RIS3), which defines national priorities for a knowledge-based structural transformation. RIS3 is part of the EU Cohesion Policy for 2014-2020 and a precondition for receiving financial support from the European Union's Regional Development Fund (ERDF).[1] In particular, RIS3 largely determines the distribution of ERDF funds across different areas. The European Union considers the Digital Agenda a core instrument for the implementation of a RIS3.

Latvia's Smart Specialisation Strategy sets three directions for economic transformation: 1) change in the production and export structure of traditional economic areas; 2) future growth areas where products and services with high added value exist or may appear; and 3) areas with significant horizontal impact contributing to national economy transformation. The strategy also determines several key priorities including more efficient use of raw materials, the creation of new materials, wider use of non-technological innovations, the development of a modern ICT system in the private and public sector, and an advanced knowledge base and human capital in areas where Latvia has a comparative advantage of importance to the process of transformation (MoES, 2013a).

The government identified five Smart Specialisation areas in line with three directions. **Knowledge-intensive bioeconomy** is a strategic area for the transformation of traditional sectors. **Biomedicine, medical technologies and biotechnology** and **Smart materials, technology and engineering** are areas with high value added and high growth potential. **Advanced ICTs** and **Smart energy** are horizontal enablers of structural transformation across economic sectors.

Several niches of competitiveness were highlighted within each of the specialisation areas (Table 6.1). Table 6.2 summarises the distribution of available funds across the different Smart Specialisation areas and funding mechanisms for the years 2014-18.

The selection of Smart Specialisation areas followed several rounds of discussions with entrepreneurs, industry associations and academia in June and July 2013. An initial assessment found that a strong product portfolio and a skilled labour force already existed in forestry and wood processing, agriculture and food as well as metalworking and mechanical engineering. High export potential was identified for woodworking, the food industry, manufacture of metal and its products, and the chemical industry, as well as information and communication services. The export of health services, while small at the time, was also considered promising. Significant patent activities were identified in the fields of surface technologies and coatings, materials, engines, turbines pumps, nano-science, audio-visual technology, health, pharmacy, and chemistry and wood chemistry, as well as selected fields of IT and management methods. Finally, the assessment highlighted research specialisation in the material sciences, biotechnology, ICT, energy and transportation technology (MoES, 2013a).

Table 6.1. Latvia's Smart Specialisation areas

Specialisation area (RIS3)	Potential specialisation niches (as of 2014)	Related industries (NACE Rev. 2)
Knowledge-intensive bioeconomy	Sustainable and productive forest growing in changing climatic conditions; Full use of wood biomass for chemical processing and energy; Innovative, risk-reducing plant and animal breeding technologies; Development of innovative high-value added niche products from wood, traditional and unconventional agricultural plant and animal raw materials; Technological solutions for the use of plant and animal breeding and processing by-products; Food safety	A – Agriculture, forestry and fishing: A.01 – Crop and animal production, hunting and related service activities; A.02 – Forestry and logging; A.03 – Fishing and aquaculture C – Manufacturing: C.10 – Food products; C.11 – Beverages; C.16 – Manufacturing of wood and of products of wood and cork, except furniture; articles of straw and plaiting materials; C.17 – Paper and paper products; C.20 – Chemicals and chemical products; C.23 – Other non-metallic mineral products; C.27 – Electrical equipment; C.28 – Machinery and equipment n.e.c. M – Professional, scientific and technical activities: M.74 – Other professional, scientific and technical activities
Biomedicine, medical technologies and biotechnology	Chemical and biotechnological methods for the production of pharmaceutical and bioactive substances; Development and research of human and veterinary medicinal products; Molecular and individualised treatment and diagnostic methods and cell technology; Functional foods, therapeutic cosmetics and bioactive natural substances	C – Manufacturing: C.10 – Food products; C.20 – Chemicals and chemical products; C.21 – Basic pharmaceutical products and pharmaceutical preparations; C.26 – Computer, electronic and optical products; C.26.6 Manufacture of irradiation, electromedical and electrotherapeutic equipment; C.32.50 Manufacture of medical and dental instruments and supplies Q – Human health activities
Smart materials, technology and engineering	Implant materials, composite materials, thin layers and coatings, equipment, machinery and working machines, glass fibre products and smart glass-based materials	C – Manufacturing: C.20 – Chemicals and chemical products; C.23 – Other non-metallic mineral products; C.25 – Fabricated metal products, except machinery and equipment; C.28 – Machinery and equipment n.e.c., C.32 – Other manufacturing
Advanced ICT	Innovative knowledge management, system modelling and software development methods and tools; Innovative sectoral ICT hardware (hardware) and software (software) applications; Cyber-physics systems, language technologies and the semantic web; Bulk data and knowledge infrastructure; Information security and quantum computers; Computer system testing methods	J – Information and communication technologies: J.61 – Telecommunications; J.62 – Computer programming, consultancy and related activities; J.63.1 – Data processing, hosting and related activities; web portals; J.58.1 – Software publishing; C.26.1 – Manufacture of electronic components and boards; C.26.2. Manufacture of computers and peripheral equipment; C.26.3. Manufacture of communication equipment; C.26.4. Manufacture of consumer electronics; C.26.8. Manufacture of magnetic and optical media
Smart energy	Development of smart grids and demand-supply systems, smart buildings, home, appliances and home automation systems; Development of next-generation technologies for energy from renewable energy sources; Increasing energy efficiency – energy efficiency of building structures, energy efficiency of residential infrastructure elements; Sustainable energy for transport – new technologies, accelerating their implementation, electric mobility	C – Manufacturing: C.27 – Electrical equipment; C.28 – Machinery and equipment n.e.c.; C.29 – Motor vehicles, trailers and semi-trailers D – Electricity, gas, steam and air conditioning supply: D.35 – Electricity, gas, steam and air conditioning supply F – Construction: F.41 – Construction of buildings; F.43 – Specialised construction activities J – Information and communication technologies: J.62 – Computer programming, consultancy and related activities

Note: ICT = information and communication technology; n.e.c. = not elsewhere classified.

Source: European Commission (2018c), "Latvia – S3 priorities as encoded in the 'Eye@RIS3' Tool", *https://s3platform.jrc.ec.europa.eu/regions/LV/tags/LV* (accessed on 30 September 2019).

Latvia's selection of Smart Specialisation areas has a rather strong focus on manufacturing activities. Services are explicitly considered only as IT services in the ICT specialisation area. Services related to well-being or social innovation are not considered. This differs from many other EU countries, including Denmark and Estonia, which have explicitly included health services or social work activities as Smart Specialisation areas, and makes Latvia's Smart Specialisation Strategy appear somewhat one-sided (European Commission, 2012b).

Each Smart Specialisation area is supported by a number of competence centres and clusters (Table 6.3). Competence centres are commercial entities founded by enterprises and research organisations, which manage and finance R&D activities with potential commercial value. They play a crucial role in improving the potential for exchange between firms and research organisations. Clusters are membership organisations in particular economic fields that aim to create positive externalities for members through network activities. In the context of innovation systems, clusters usually include three types of members (triple-helix), namely private, academic and public entities (e.g. universities and research institutions). Clusters and cluster policies are considered to be among the key building blocks in developing and implementing RIS3 (European Commission, 2013).

Table 6.2. Funding instruments for Smart Specialisation, 2014-18

In EUR

Source	National government		Funding instruments of the Ministry of Education and Science		EU Innovation and research programme	Funding instruments of the Ministry of Economics		Total
			ESIF (e.g. ERDF, ESF)		Horizon 2020	ESIF (e.g. ERDF, ESF)		
	ERA-NET	Fundamental and applied research programme	Post-doctoral research	Practical-oriented research	Horizon 2020	Research results commercialisation	Competence centres	
Bioeconomy	..	3 003 297	3 255 695	3 349 101	4 456 544	778 245	9 752 819	**24 595 701**
Biomedicine	2 539 607	4 996 572	6 155 076	19 683 916	2 329 968	2 302 933	7 871 315	**45 879 387**
Smart energy	..	5 378 043	12 404 929[1]		12 419 688	4 050 0081[1]		**34 252 668**
Smart materials	..	8 012 905	5 352 240	15 722 087	2 994 482	3 713 511	16 399 223	**52 194 448**
ICT	..	3 494 203	3 813 470	5 238 442	7 511 618	2 095 685	10 780 921	**32 934 339**
Total	**2 539 607**	**24 885 020**	**74 974 956**		**29 712 299**	**57 744 660**		**189 856 543**

1. This number refers to total funds from ESIF.

Note: .. = not available; ICT = information and communication technology.

Source: OECD, based on data from the MoES.

Table 6.3. Smart Specialisation: Competence centres and clusters

Specialisation area (RIS3)	Competence centres	Clusters (launched since 2017)
Knowledge-intensive bioeconomy	Latvian Food Competence Centre (LFCC), Forest Sector Competence Centre (FSCC)	Food Products Quality Cluster, Latvian Wood Construction Cluster, CLEANTECH Latvia (cross-sectoral), Smart City Cluster (cross-sectoral)
Biomedicine, medical technologies and biotechnology	Pharmacy, Biomedicine and Medical Technology Competence Centre (PBMTCC)	Life Science Cluster of Latvia
Smart materials, technology and engineering	Mechanical Engineering Competence Centre (MECC), Smart Materials and Technology Competence Centre (SMTCC)	Metal working Cluster, Green and Smart Technology Cluster (cross-sectoral), Printing and Media Technology Cluster
Advanced ICT	IT Competence Centre (ITCC), LEO Research Centre (LEO)	Information Technology Cluster
Smart energy	Smart Engineering, Transport and Energy Competence Centre (SETECC)	Latvian Electronics and Electrical Engineering Cluster

Source: OECD, based on MoES (2018), *Informative Report: Monitoring of Smart Specialization Strategy*, *https://s3platform.jrc.ec.europa.eu/documents/20182/0/RIS3_progress+report_LV_2018.pdf/940176c6-b886-4213-9f18-75c20251bfb9*.

In 2018, the government conducted an initial assessment of the implementation of the Smart Specialisation Strategy, and concluded that Latvia's competitive advantage still relies largely on low labour costs and natural resources. Investments in research and development as a percentage of GDP declined slightly between 2010 and 2016, while labour productivity in manufacturing increased slightly, but remained below expectations. In addition, Latvia moved from the modest to the moderate performance group in the European Innovation Index, although this result was based largely on EU support during the previous funding round (2007-13). The assessment reported positive developments with regard to science publications, the educational attainments of young adults (aged 30-34), research fragmentation and export of high technology goods (MoES, 2018). However, the assessment did not address the performance of particular specialisation areas or research fields.

To better assess the effectiveness of invested funds, an RIS3 monitoring system was put in place in 2016. The results will be used to shape the next iteration of the Smart Specialisation Strategy (2021-2027), which will shift the focus from fostering loosely related product niches (Table 6.1) to developing a smaller selection of ecosystems with potential for comparative advantages. An important difference is that the new approach better accounts for the crucial role of different ecosystem players as well as upstream and downstream activities (i.e. the value chain).

At present, the Latvian government has identified three ecosystems for development: biomedicine, smart materials and smart cities.[2] Out of these, the Smart City is the only ecosystem currently not explicitly linked to any of the existing specialisation areas. However, there are significant overlaps

between the Smart City concept and the specialisation areas of Smart Energy (including mobility) and Biomedicine (including remote healthcare monitoring). Sustaining clear links to existing Smart Specialisation areas can be critical to ensure continuity. As the Latvian definition of the Smart City concept explicitly highlights measures that allow for timely anticipation and prevention of potential challenges, such as energy shortages, heat losses or sewer leaks, the following sections, which provide an assessment and recommendations for different Smart Specialisation areas, treat the Smart City ecosystem within the area of Smart Energy. Overarching policy recommendations that arise from the following sections can be summarised as follows.

First, public support for Smart Specialisation should be better targeted at ecosystems with high growth potential, taking into consideration the whole value chain, from research to commercialisation. In the past, the Smart Specialisation Strategy has provided support to too many distinct product niches without prioritisation. This has resulted in funds being spread too thinly. The new ecosystem approach can help to improve targeting, and the following sections provide some indications of where potential might lie.

Second, Latvia should better leverage the ICT Smart Specialisation area as an enabler of innovation in other specialisation areas. As digital technologies generate positive spill-overs across all economic activities, the share of spending on ICTs in total spending on Smart Specialisation (Table 6.2) should be increased significantly.

Third, while fostering innovation is at the core of the Smart Specialisation Strategy, encouraging the uptake of existing technologies is an important complementary strategy. In particular, wider dissemination of general purpose technologies such as ICTs is crucial, because it enables more firms to innovate (OECD, 2019j). This is particularly important for services firms, which should be accorded a more prominent role in Latvia's Smart Specialisation Strategy.

Box 6.5. Smart Specialisation: Overarching recommendations

- Concentrate funding for Smart Specialisation on ecosystems with high potential.
- Increase the share of RIS3 funding devoted to ICTs and target applications of high relevance for other Smart Specialisation areas.
- Complement the Smart Specialisation Strategy with measures to broaden and diffuse innovation, in particular by fostering the uptake of digital technologies.

Latvia's bioeconomy strategy

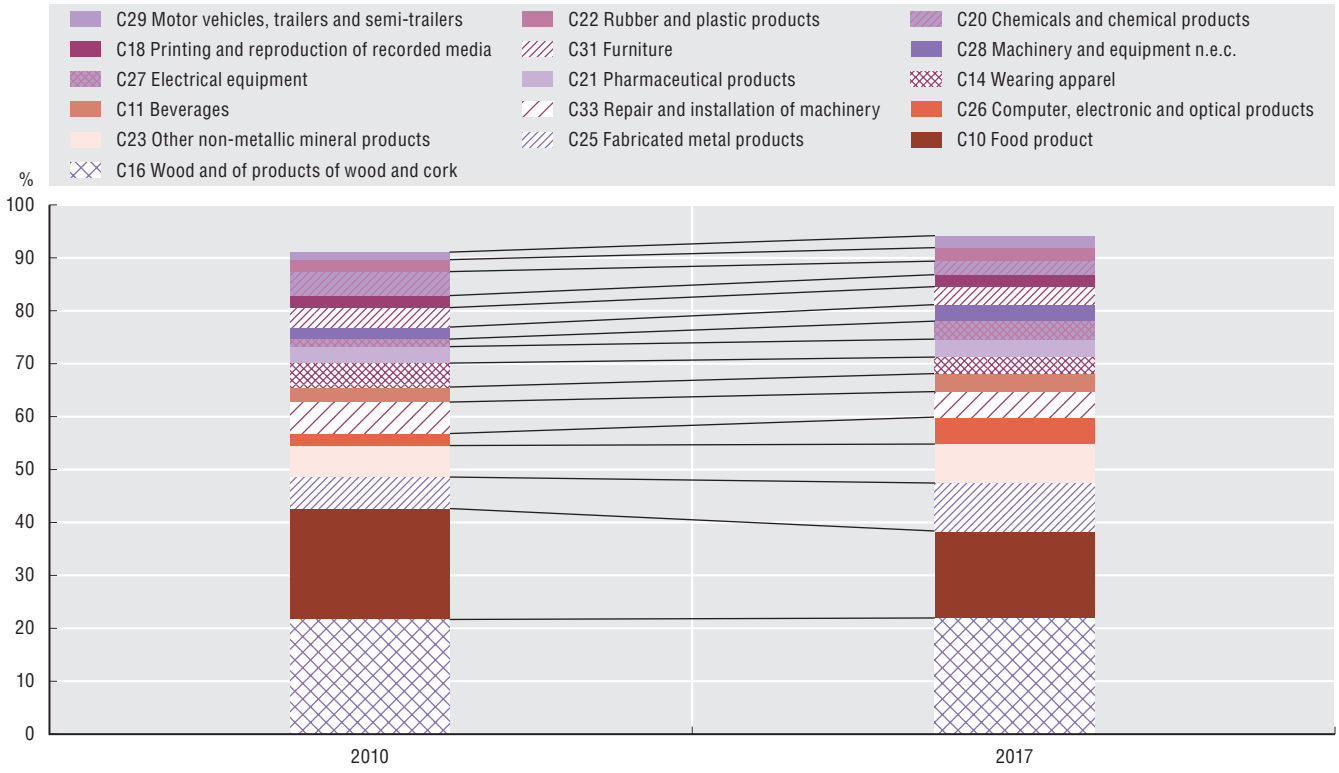
The bioeconomy involves the use of renewable feedstock to produce goods and services. It encompasses a wide range of sectors and activities, including chemicals, food, agriculture, dairy, forestry, pulp and paper, waste management and others. Accordingly, the term "bioeconomy" does not necessarily convey a particular notion of technological intensity. Traditional forestry is as much a part of the bioeconomy as the genetic manipulation of biomass and synthetic biology. In Latvia's Smart Specialisation Strategy (RIS3), the knowledge-intensive bioeconomy relates to some of the more traditional sectors, including agriculture and forestry, as well as related manufacturing sectors such as food or products made from wood. This specialisation area also includes some knowledge-intensive activities such as chemical wood processing or renewable energy from bio-resources. For these sectors, RIS3 emphasises an extension of the product space and a gradual upgrade towards higher value-added products.

Comparative advantages in the bioeconomy are based on abundant resources rather than innovation

In 2017, agriculture, forestry and fishing, with manufacturing activities related to food and wood products, accounted for close to 9% of Latvian total value added. Traditional bioeconomy sectors thus form an important part of the economy. The significance of the bioeconomy is particularly pronounced in the manufacturing sector, where products made of wood and cork (excluding furniture but including straw and plaiting materials) as well as food and beverages account for 43% of total value added (Figure 6.12). Over time, the contribution of wood and related manufacturing activities increased slightly, from 21.6% in 2010 to 22.1% in 2017, but declined significantly for the food sector, from 20.9% to 16.4%.

Figure 6.12. Contribution of the bioeconomy to manufacturing value added, 2010 and 2017

As a percentage of total manufacturing value added



Note: n.e.c. = not elsewhere classified.

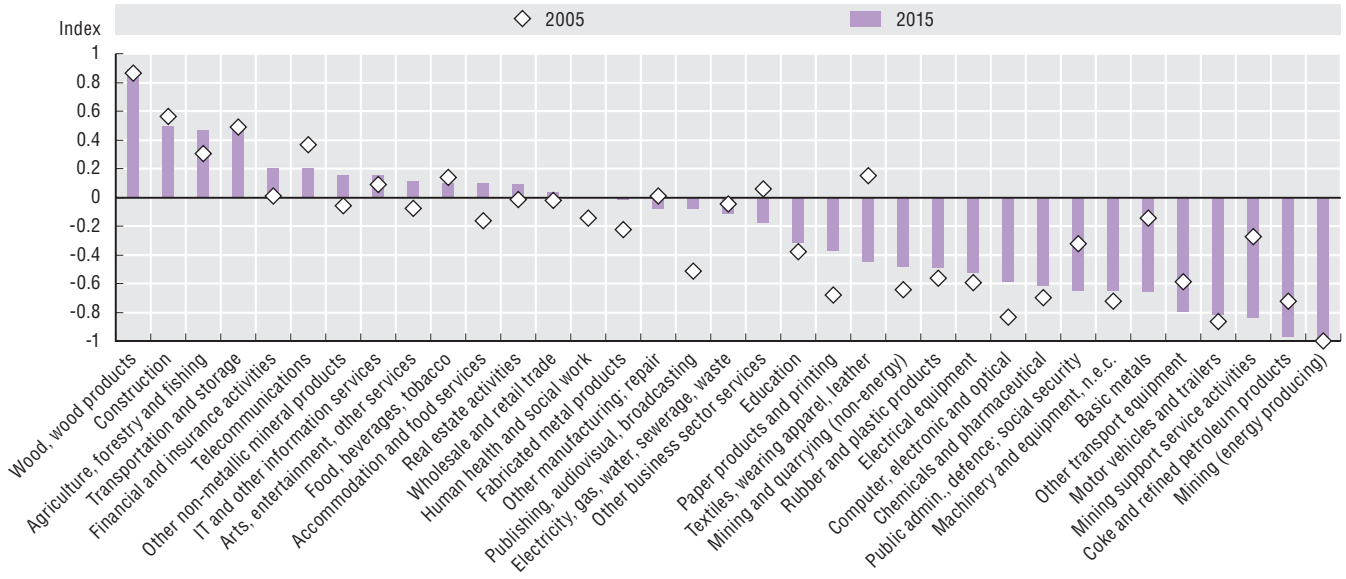
Source: CSBL (2020a), *IKG10_060 Total Gross Value Added by Kind of Activity (NACE Rev. 2)* (database), *https://data1.csb.gov.lv/pxweb/en/ekfin/ekfin__ikp__IKP__ikgad*.

Latvia has substantial revealed comparative advantages (RCAs) in traditional bioeconomy sectors.[3] In 2015, the share of wood and wood products in Latvia's total exports was 14 times higher than the corresponding share in world exports. This accounts for both direct exports of wood and wood products, as well as indirect exports of wood products embedded as intermediates in other products (Figure 6.13). Furthermore, compared to 2005, the RCA has become larger over time, implying increasing specialisation. RCAs for agriculture, forestry and fishing are also significant, with the sector's share in total exports in 2015 being over 2.8 times higher than in other countries.

However, while Latvia is still exporting more food products than other countries, and labour productivity has kept increasing, food exports have suffered substantially from a Russian embargo that began in 2014 (MoE, 2018b).

Latvia's traditional bioeconomy exports concentrate on low-value added products. In the food sector, high-value added exports are stifled by a lack of processing capacity and value chain inefficiencies (OECD, 2019g). For example, the Latvian food processing industry today includes fewer large businesses and more numerous small ones than a decade ago, and a large share of the increasingly organic production is being sold to conventional processors (e.g. more than half for organic milk and eggs and one-third for meat and cereals). For the forestry value chain, a significant share of exports is still determined by products such as sawn wood, fuel wood, wood in the rough or wood charcoal, while products higher up the value chain, including furniture or paper, remain more limited. However, over time there has been a significant increase in the export of products higher up the value chain, such as wood panels or wooden houses, implying that the value of exports has increased compared to total wood production (Figure 6.14).[4]

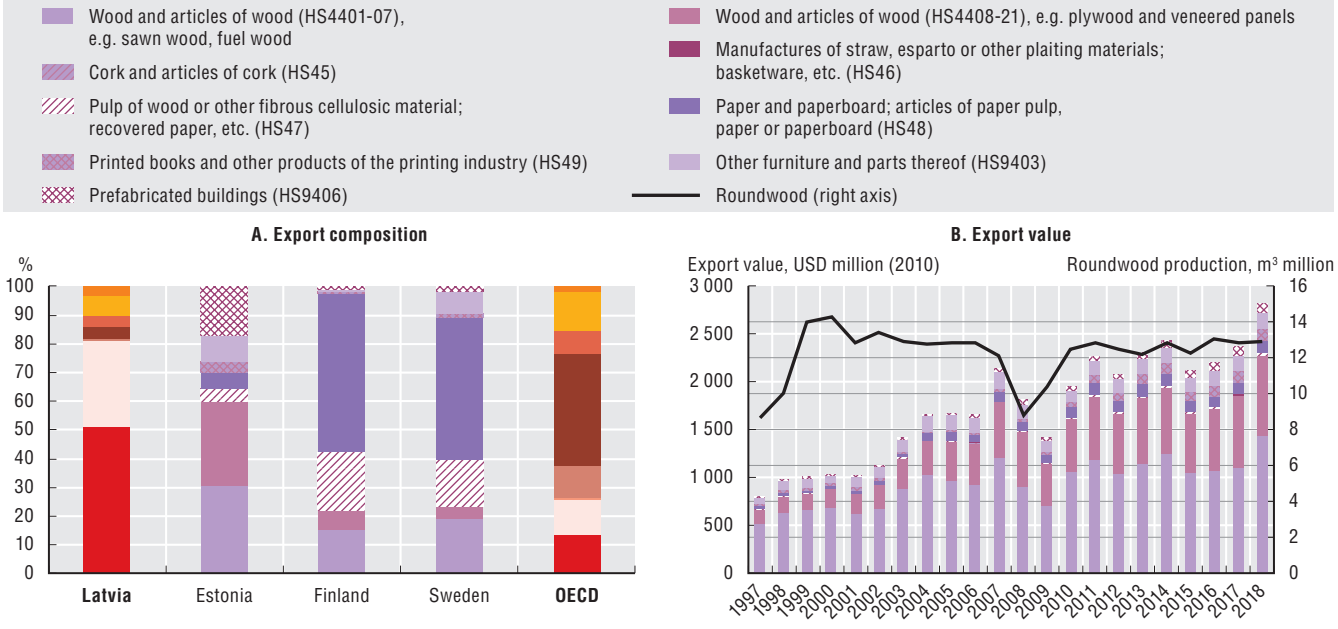
Figure 6.13. Latvia's revealed comparative advantage, 2005 and 2015



Notes: n.e.c. = not elsewhere classified. Revealed comparative advantage (RCA) of exports in value-added terms. The calculation in value-added terms takes into account GVC linkages. In particular, exports of a given sector are considered irrespective of whether they are directly exported or embodied in the exports of downstream sectors. See Miroudot and Cadestin (2017) for details. The RCA in the figure is normalised to [-1;1]. To obtain the original RCA values referred to in the text, the formula (x+1)/(1-x) needs to be applied.

Source: OECD (2020d), "Trade in value added", *https://dx.doi.org/10.1787/data-00648-en* (accessed on 27 February 2020).

Figure 6.14. Value added of forestry products in Latvia and selected OECD countries



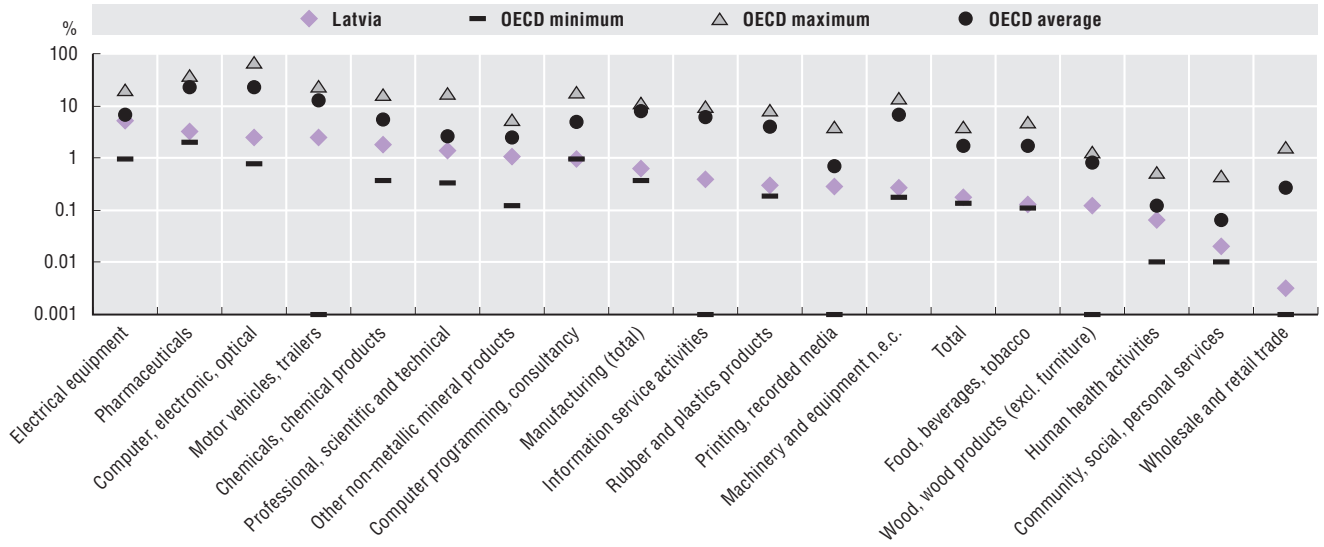
Note: The export values (current USD) in panel B have been deflated with US CPI index (2010).

Sources: WITS/UN Comtrade (2020), *UNSD Commodity Trade* (database), *http://wits.worldbank.org* (accessed on 4 February 2020); FAO (2020), *Forestry Production and Trade* (database), *www.fao.org/faostat/en/#data/FO/visualize* (accessed on 20 May 2020).

Latvia's bioeconomy significantly trails OECD countries with regard to R&D. In 2015, R&D expenditures of Latvian firms as a share of value added were equal to 0.13% in food manufacturing and 0.12% in the wood products industry, compared to an OECD average of 1.76% and 0.81%, respectively (Figure 6.15). This seems to confirm the assumption that output and export growth in these sectors is based on an abundance of natural resources rather than innovation and productivity.

Figure 6.15. R&D expenditure by industry in Latvia relative to the OECD, 2015

As a percentage of each industry's value added



Note: Logarithmic scale. Averages are weighted using value added in purchasing power parities (GDP). Data for Chile, Estonia, Hungary, Japan, Lithuania, Portugal and the United States are from 2014. Data for France are from 2016.

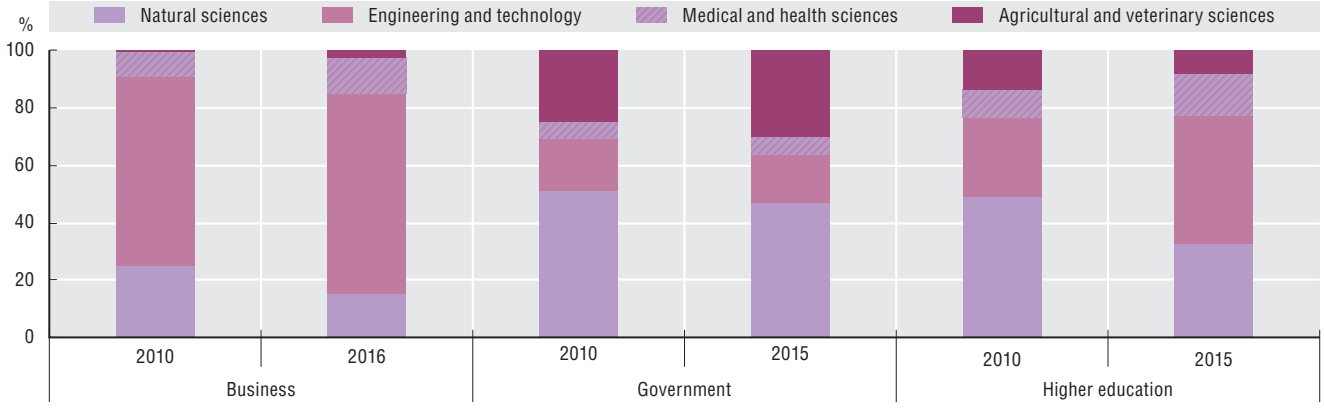
Sources: OECD (2020e), "Research and development statistics: Business enterprise R-D expenditure by industry – ISIC Rev. 4", *https://dx.doi.org/10.1787/data-00668-en* (accessed on 13 March 2020); OECD (2020f), "STAN Industry ISIC Rev. 4", *https://dx.doi.org/10.1787/data-00649-en* (accessed on 24 February 2020).

The government has strengthened research in the bioeconomy but technology transfer to smaller firms remains weak

Over the past decade, the government has made substantial efforts to enhance innovation in traditional bioeconomy sectors. Between 2010 and 2015, government R&D expenditures on agricultural and veterinary sciences increased by close to EUR 5 million, (i.e. from 25% to 30% of government R&D expenditure in the natural sciences and engineering) (Figure 6.16). However, government spending increases (e.g. on public research facilities) were not accompanied by additional funding for HEIs. Potentially, this could negatively impact on availability of scientific talent in the future.[5]

Figure 6.16. Latvia's R&D expenditure in natural sciences and engineering, by performing sector

As a percentage of total R&D expenditure in natural sciences and engineering performed by each sector



Source: OECD (2020g), "Research and development statistics: Gross domestic expenditure on R-D by sector of performance and source of funds", *https://dx.doi.org/10.1787/data-00189-en* (accessed on 26 February 2020).

The government has also taken steps to enhance co-ordination among research institutions. In 2014, 14 scientific institutions in agriculture, food, forestry and related sectors, including woodworking and wood chemistry, formed the Strategic Association for Bioeconomy Research. Following a consolidation process in 2015, the association now consists of eight institutions. These include: the Latvian University of

Life Sciences and Technologies (LLU); three independent institutions under the university's supervision, namely the Institute of Horticulture, the Institute of Agricultural Resources and Economics, and the Latvian Plant Protection Research Centre; the Institute of Food Safety, Animal Health and Environment (BIOR); the Latvian State Forest Research Institute (Silava); the Institute of Wood Chemistry; and the Forest and Wood Products Research and Development Institute (MeKA).

Over time, the association has seen a substantial increase in the number of research personnel, from 242 in 2013 to 359 in 2016 (MoA, 2018). The share of cited publications in the field of agricultural and food science in all Latvian publications increased significantly from 11% in 2007-12 to 16% in 2013-16 (OECD, 2019g). However, revenues from the transfer of intellectual property rights or other research services provided to third parties, decreased in 2016-15 from EUR 4.7 million to EUR 4.2 million, below their level in 2013. This suggests that there is room for Latvia to enhance knowledge transfer from publicly funded research into commercial applications. The critical role of more knowledge transfer mechanisms has been explicitly acknowledged in Latvia's Bioeconomy Strategy 2030, which the government published in 2018. In particular, the strategy highlights slow and fragmented knowledge transfer as a main obstacle to value-added upscaling in production (MoA, 2018).

An important step towards better collaboration between scientific institutions and firms has been the creation of competence centres in different research areas. By the end of 2018, 149 firms had benefited from one of the eight competence centres, of which 31 were supported by the Latvian Food Competence Centre and 13 by the Forest Sector Competence Centre. Private investment complementing state aid for R&D projects totalled EUR 1.9 million for the food sector and EUR 2.3 million for the forest sector. However, industry stakeholders have noted that the limited capacity of competence centres represents a bottleneck for potential new projects. More importantly, the high research intensity of the projects makes the programme unsuitable for SMEs.

The government should strengthen mechanisms for the commercialisation of applied research results that are better suited for SMEs, such as the Technology Transfer Programme. Instruments to promote research commercialisation received only 3.2% of total spending in the Smart Specialisation area (Table 6.2). Additionally, the Technology Transfer Programme has only a single contact point for the bioeconomy, at the Latvian University of Life Sciences and Technology (LLU). The Technology Transfers Offices Flanders, a joint initiative by five Flemish universities, provides a good example of how different universities and research institutes can co-operate to provide online access to all the available knowledge and technology within different institutions (Box 6.6).

Box 6.6. Technology Transfer Offices (TTO) Flanders

TTO Flanders is a joint initiative of five Flemish universities: Ghent University, the University of Antwerp, KU Leuven, Vrije Universiteit Brussel and Hasselt University. The technology transfer offices (TTOs) of these universities are responsible for the transfer of knowledge and technology from universities and associated university colleges to private and public partners. This includes establishing contact with industry, offering legal support related to contracts, promoting education activities for engagement, offering protection of intellectual property and supporting start-ups and spin-offs.

The joint initiative provides a unique point of contact (*www.ttoflanders.be*) for industries looking for research expertise and licensing opportunities, aimed at better valorisation of available knowledge and technology. It fosters collaboration between the five different TTOs and strengthens their performance by developing common means and sharing best practices. The universities and university colleges involved hope that the initiative will help the Flemish TTOs become a more effective player on the European and international innovation scene.

TTO Flanders offers technologies in areas such as food and agriculture, health, materials and chemistry, ICT and electronics, and cleantech and energy, and provides links to the relevant centres of expertise. The website is available in English and directs customer questions to the right person or research centre. The estimated budget expenditure per year ranges from EUR 1 million to 5 million.

Sources: OECD (2019k), Benchmarking Higher Education System Performance, Higher Education, *https://dx.doi.org/10.1787/be5514d7-en*; European Commission/OECD (2020), STIP Compass: International Database on Science, Technology and Innovation Policy (STIP), *https://stip.oecd.org*.

Latvia should target high-value added forestry products and exploit synergies with material sciences

The wood processing sector has outperformed the food sector along several dimensions in recent years, including value-added contributions, revealed comparative advantage and R&D spending by the private sector (see above). Taken together with the absolute advantage of vast amounts of forest areas, this suggests high potential for a competitive ecosystem within the wood processing sector in Latvia.

In order to remain competitive on international markets, Latvia's forestry sector needs to move up the global value chain. With the global use of paper falling, competition from topical and sub-tropical regions rising, and increasing automation along the value chain, traditional wood product manufacturers in Latvia, Finland or Sweden will find it increasingly difficult to compete without innovation (OECD, 2017b).

For Latvia, signs of positive dynamics are emerging in areas where material science and new technologies are being used to transform raw material into exportable products. For example, in a recent research collaboration, commissioned by the Forest Sector Competence Centre, the Latvian State Institute of Wood Chemistry (IWC) and joint-stock company Latvjas Finieris, a producer of birch plywood, have developed a new method to obtain Betulin – a substance responsible for the white colour of birch bark – on an industrial scale. The unrefined Betulin is aimed at the cosmetics market and by-products of the process can be used to replace formaldehyde as a glue for wood composites or as mineral fertilisers.

The case of Betulin, which is known for its positive health effects, is an example of potential synergies not only with the Smart Materials specialisation area, but also with the Biomedicine ecosystem. For example, Riga Technical University (RTU) and Rīga Stradiņš University (RSU) have been co-operating since 2016 to obtain a bioactive chemical compound with anticarcinogenic properties from Betulin. RTU and LLU are researching additional applications of the refined form of Betulin, including its use in medical cosmetics to support skin regeneration or as an additive in food to prolong the storage life of milk or meat products (Vaivare, 2018a).While it is currently unknown how marketable these products will be, Latvia is likely to benefit from the knowledge created across these different projects.

Latvia's Bioeconomy Strategy should have a stronger digital focus

Latvia's Bioeconomy Strategy 2030 does not have a digital focus in spite of the fact that the whole ecosystem, from the extraction of raw material to food and wood manufacturing, is ripe for digitalisation. While there is no plan at present to update the strategy, consideration of how best to govern the digital transformation in agriculture, forestry and food will become increasingly important. As a first step, Latvia should measure the digital transformation in the bioeconomy, starting with an analysis of access and use for basic digital technologies, as well as more advanced tools specific to agriculture, forestry or food production. Recent experience in the food manufacturing sector suggests that digital readiness remains low, with firms in the sector experiencing significant difficulties navigating even basic digital management tools (PPKK, 2019).

Several recent initiatives are trying to fill these gaps. For example, the Latvian IT Cluster and the Food Product Quality Cluster form part of DIGICLUSTERS, a European Cluster Collaboration Platform sponsored by the European Union, which focuses on enhancing the competitiveness of SMEs in the agro-food packaging sector. Latvia also participates in SmartAgriHubs, a EUR 20 million EU Horizon 2020 instrument fostering the development and adoption of digital solutions in farms across Europe. The project, which runs from 2018 to 2022, envisages the establishment of an innovation portal and catalogue for farmers and agribusiness to map existing digital technologies and facilitate the exchange of best practices among network participants (e.g. start-ups, SMEs, business and services providers, technology experts, etc.).

LIKTA runs a project entitled Training of Small and Micro Entrepreneurs for Development of Innovations and Digital Technologies in Latvia (Project 1.2.2.3/16/I/002) under the responsibility of the Ministry of Economics. The initiative, co-funded by the European Union (EUR 2 001 937) and the private sector (EUR 762 600), provides training in three areas: digital technology (e.g. cloud services or security), digitalisation of internal company processes (e.g. financial management and marketing), and digital tools for production and service development (e.g. CRM). The project aims to reach 6 200 managers and employees by December 2020.

There are, however, no specialised training courses offered on digital tools for the bioeconomy. In the agricultural sector, the Latvian Rural Advisory and Training Centre (LLKC) offers several courses for rural entrepreneurs via its distant learning platform (LLKC Talmaciba). However, none of the courses currently has a digital focus. The government should use LLKC to provide more specialised training on the use of digital technologies in agriculture, such as precision agriculture or drones. For example, the National Service for Rural Apprenticeship (SENAR) in Brazil has offered free courses on drone use in agriculture since 2016, including on regulation (SENAR, 2016).

The government should foster open data policies to enhance digital transformation in the agro-food sector

The government could also further leverage existing information systems to disseminate advanced applications and data tools among farmers and other rural entrepreneurs, as well as in fisheries. Two systems that seem particularly promising in this regard are the Electronic Application System (EAS) of the Rural Support Service and the Latvian Fisheries Integrated Control and Information System (LFICIS).

The EAS was developed in 2007 to simplify the application process for EU and state support. Over time, additional features were added and use of the system became obligatory in 2016. EAS now also links to services from other agencies with access to geospatial data provided through the Web Map Service (WMS) and the Web Feature Service (WFS). In 2015, the programme received the UN Public Service Award for the category "Promoting Whole of Government Approaches in the Information Age" and was also the winner of the 2017 World Summit on the Information Society (WSIS) Prize in the field of e-agriculture. The LFICIS is operated by the MoA and links several databases and data tools. Since June 2018, the system also contains a product traceability module, which tracks fisheries products from landing to retail and export. It currently provides information to several government agencies, including for fisheries and food safety control and customs, as well as private sector market participants, including fishermen, wholesalers and consumers.

Enabling the private sector to openly access selected data available in the EAS and the LFICIS, and to develop and append additional value-added services, could also help Latvia attract innovative service providers. For example, in 2014 the French co-operative InVivo acquired a majority stake in SMAG, an agricultural software provider, to develop farm management applications based on shared data from its members.

Fostering online platforms in the bioeconomy can also bring benefits in other areas, such as in the case of open software platform FIspace. Created by a consortia of universities and firms with the support of EU funding, FIspace fosters the sharing of farming and food supply chain data in order to enhance business-to-business collaboration (Paunov and Planes-Satorra, 2019). In Brazil, the online platform Uller offers a peer-sharing solution for agricultural machinery and constitutes an interesting example of how digital technologies can help overcome the financial restrictions facing agricultural producers. Applications for the delivery of better policies are also viable (Box 6.7).

The Latvian government should also speed up the digitisation of spatial data, including the plant, agrochemical and soil data of the State Plant Protection Service. In the context of Latvia's Data Driven Nation (DDN) Memorandum of Understanding, the Information Society Development Council has agreed to make available a limited number of geospatial datasets for fee-free usage. However, the business model for data sharing should be reconsidered (Ozols, 2018). An important barrier to the wider release of public data is that a significant budget share of some public institutions (e.g. the State Land Service) is derived from the provision of data. The Australian Productivity Commission in 2017 issued a detailed report examining the benefits and costs of different options for sharing data between public entities, individuals and the private sector, which could serve as guidance, including on regulatory approaches and principles to address the concerns of data owners and enhance trust in data sharing initiatives (Productivity Commission, 2017). With regard to funding support for public sector data releases, the report considers several options, including a re-prioritisation of existing agency budgets, additional earmarked funding through the government or a reward system where agencies are rewarded for data releases that result in research outputs of public interest. The report further recommends that agencies provide annual reports on the proportion of datasets made publicly available, shared and not available for release. It suggests that a central office (National Data Custodian) could take overall responsibility

for the implementation of data management policy and accredit other entities to enhance linkages between different datasets. The OECD (forthcoming) provides additional examples and best practices with a particular focus on the regulatory aspects of data governance in agriculture, which could be informative for the discussion in Latvia.

Box 6.7. Leapfrogging potential: Big data for better policies in agriculture and forestry

Recent digital innovations provide opportunities to deliver better policies for the agriculture sector by helping to overcome information gaps and asymmetries, lower policy-related transaction costs, and enable people with different preferences and incentives to work better together (OECD, 2019r).

In Latvia, the research project "Evaluation of land use optimisation opportunities in Latvia in the context of climate policy" has raised the prospect of better-targeted policies. Researchers from the Latvian University of Life Sciences and Technologies (LLU) aggregated spatial data from various sources to assemble fine-grained maps (parcel level) of both agricultural and forestry land use in Latvia. The data contain a range of information including soil type, farm size or melioration status in the case of agriculture, and species, age group or site quality in the case of forestry. The specific characteristics of each parcel can be linked to data on economic (e.g. profit), social (e.g. labour input), climate (e.g. greenhouse gas emissions) or biodiversity (e.g. bird habitat quality) measures to better understand and potentially forecast performance relationships. The study has aimed to optimise the use of agricultural and forest land capacity assessments, and could help policy makers devise more coherent land-use related policies, including financial incentives that simultaneously address different policy objectives (e.g. environmental and social).

Latvia's State Forests (LVM), the publicly owned company that administers Latvia's state-owned forests, has provided financial support for the research and is already using the tool to maximise profits while keeping the forest inhabitable. However, additional uses seem viable, for example to enhance the targeting of other policy measures (e.g. to achieve reduction in greenhouse gases). LVM, through its informatics division, has proven quite successful in the development of innovative software solutions. For example, LVM GEO provides flexible access to geospatial information via desktop, browser or mobile apps (online and offline). The database integrates land and forestry data with other data sources, including the drainage cadastre, state road services or the nature conservation agency. The platform, which was initially developed for in-house usage, is now open to other companies and organisations, and due to its modular structure allows for several stand-alone solutions and integration with other proprietary systems.

Access to spatial data is also important for the wider adoption and usage of remote monitoring systems, including Latvia's planned pilot project on technologically enhanced fire monitoring towers or drones. In the case of drones, many agricultural and forestry applications are inhibited by current regulation which prohibits the use of drones beyond the line of sight (500 m) (Regulation No. 737). New European regulation, which entered into force in July 2019, could soon allow for more flexible uses, but will be fully applicable only after a two-year transition period. In particular, the new regulation describes a category for "specific" usage, eliminating restrictions concerning the visual line of sight, mass or altitude of operation. Most usage scenarios in agriculture would likely fall into the specific category. The Latvian government should foster fast adaptation of the new regulation. A positive signal in this regard was a drone flight conducted by Latvia's president and the president of Latvijas Mobilais Telefons (LMT) beyond the visual line of sight via the mobile network as a demonstration of the potential of the 5G ecosystem.

Biomedical research and health innovation

Biomedicine, as a Smart Specialisation area, covers medical technologies and links to sectors such as chemical and pharmaceutical industries, manufacturers of electrical and optical products as well as medical and dental instruments, and human health activities.

Box 6.8. Policy recommendations: Bioeconomy

- Strengthen the capacity of the Forest Sector Competence Centre and enhance knowledge transfer towards smaller firms by upscaling the Technology Transfer Programme and creating a single digital point of entry.
- Encourage public support for research on products high up the forestry value chain, and exploit synergies with smart materials or other Smart Specialisation areas.
- Measure digital uptake in the agro-food sector and leverage existing digital platforms, such as the Electronic Application System (EAS), by disseminating advanced applications and data tools among rural entrepreneurs and farmers. Invite private sector service providers to deliver relevant value-added services through public platforms.
- Leverage the Latvian Rural Advisory and Training Centre (LLKC) to provide specialised training on digital agriculture.
- Foster open data policies and provide easily accessible information via the relevant normative environment (e.g. via a website).

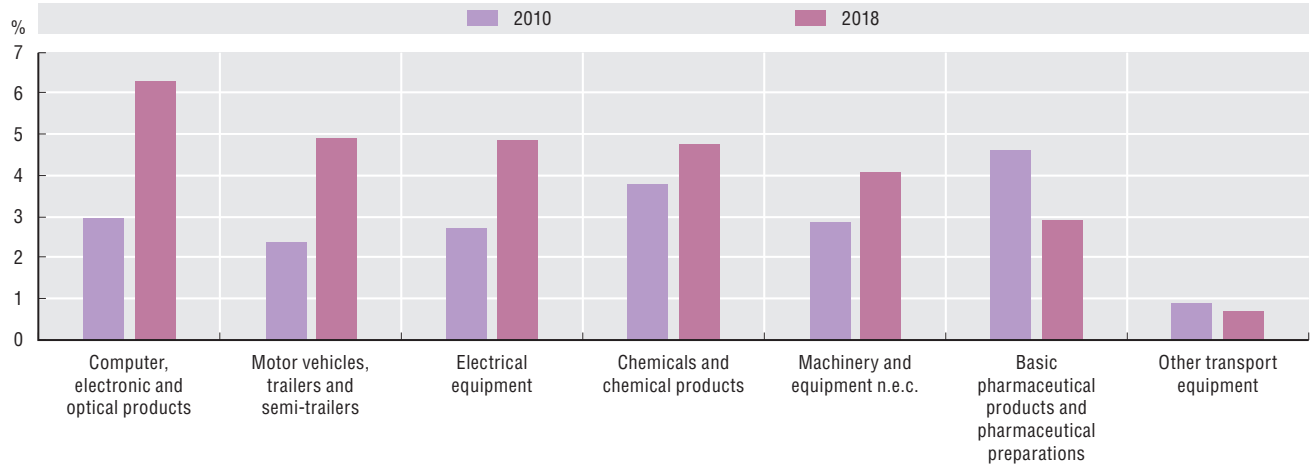
Latvia appears to be losing ground in pharmaceuticals and medical technologies

Between 1945 and 1991, Latvia emerged as one of the major producers of new drug designs and medical products in the former Soviet Union (LIDA, 2019h). Important drivers of this success were public research institutes, such as the Institute of Organic Synthesis, established in 1957, and large pharmaceutical producers such as Grindeks (1946) or Olainfarm (1972).

In 2017, the pharmaceutical sector still accounted for 3.3% of total manufacturing value added, slightly up from 3.0% in 2010 (Figure 6.12). However, over the same period the share of pharmaceuticals in total manufacturing exports diminished from 4.6% to 2.9% (Figure 6.17). Furthermore, a broader sector aggregate, encompassing also chemical industries, revealed no comparative advantage in 2015 (Figure 6.13).

Figure 6.17. Latvia's exports of high-tech and medium-high tech products, 2010 and 2018

As a percentage of total manufacturing exports



Note: The figure shows the share of high-tech and medium-high tech products in total manufacturing exports. High-tech products encompass computer, electronic and optical products as well as basic chemical products and chemical preparations. Classification based on Galindo-Rueda and Verger (2016).

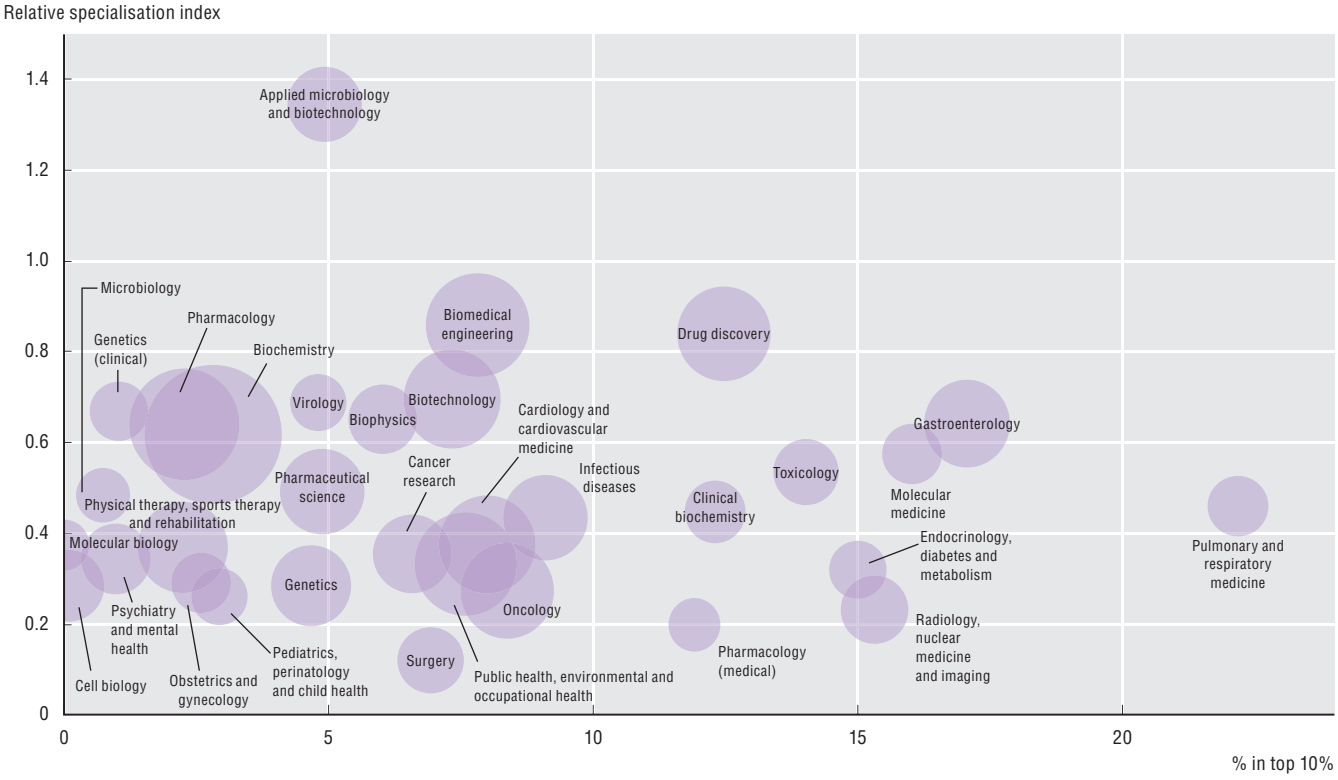
Source: CSBL (2020b), *Exports and Imports by Commodity Section and by Economic Activity (NACE Rev.2) of the Importer (thsd euro) – ATG015* (database), *www.csb.gov.lv/en/statistics/statistics-by-theme/foreign-trade/ft-nace-bec/tables/atg015/exports-and-imports-commodity-section-and*.

Several indicators point to weakening innovation in the sector. In 2015, Latvia's R&D in the pharmaceutical industry accounted for only 3.3% of value added, compared to an OECD average of 23.4% (Figure 6.15). The number of patents in pharmaceuticals and medical technologies fell from about 32% of all Latvian patents in the period 2007-11 to 19% in 2012-16.[6]

In 2014-18, the share of Latvian scientific publications in pharmaceuticals and pharmacology among the global top-10% most cited publications was 8.5%, compared to a (definitional) world average of 10%. Research excellence (i.e. more than 10% among the top-cited publications) was reached for particular subfields like toxicology (14% among the top 10% cited) and drug discovery (12.5%) (Figure 6.18).

Figure 6.18. Latvia's publications in the top 10% most cited documents

Average, 2014-18



Notes: The percentage of publications in the top 10% most cited documents is an indicator of excellence. It indicates the amount (in percentages) of a unit's scientific output included in the group of the 10% most cited papers in their respective scientific fields. The world average is 10% for the period. The Relative Specialisation Index measures relative specialisation. This index is calculated by dividing all papers in a field from country a by total production in all fields for country a. This proportion is then divided by the corresponding proportion for the world. The world average is 1. A threshold has been set and the index has only been calculated for countries with 50 or more documents.

Source: OECD calculations based on Elsevier, Scopus Custom Data, Version 5.2019.

Taking into account other fields related to the Smart Specialisation area, such as medicine, immunology, biochemistry or genetics, further suggests research excellence in areas such as pulmonary and respiratory medicine (22.2% among the top 10%), gastroenterology (17.1%) or molecular medicine (16%). However, Latvia specialised in none of these fields, implying that the contribution of the sub-field to all Latvian publications remained below the share of this field in all (world) publications.

Applied microbiology and biotechnology are the only fields related to the Smart Specialisation area for which Latvia exhibits specialisation. However, the share of excellent publications remained low (4.9% in top 10%). Additionally, while Latvian patent applications in biotechnology have been increasing from 0.2 in 2007-11 to 2.1 in 2012-16, the number is too small to determine a trend.

The government should promote innovation diffusion in the public health system while strengthening research skills

The share of medical and health sciences in total R&D expenditures in the field of natural sciences and engineering rose from 8.4% to 12.1% between 2010 and 2016, increasing from EUR 8.1 million to EUR 11.7 million, respectively. By far the largest increase can be attributed to HEIs, which increased spending from EUR 3.6 million to EUR 6.8 million. Relative to other fields in the natural sciences and engineering, spending on medical and health sciences also grew in importance for the business sector and the government (Figure 6.16). However, expenditures for both actors remained rather stable in absolute terms (EUR 3.2 million and likely below EUR 2 million, respectively).[7]

In 2014-18, biopharma and biotechnologies and translation medicine accounted for 40% and 25%, respectively, of the EUR 46 million in funds allocated under the Smart Specialisation framework. A large share of the funds for biopharma and biotechnologies was channelled through the Pharmacy, Biomedicine and Medical Technology Competence Centre (PBMTCC), where the sub-field accounted for around 95% of total spending, or around EUR 7.5 million. Translational medicine, which aims to better link laboratories, hospitals and patients, received over 62% of the H2020 funding distributed to the Smart Specialisation area.

Two of the largest H2020 grants received by Latvia not only illustrate the country's recent contributions in this area, but also highlight the relationship with digital technologies, the critical role of international co-operation and potential routes towards research commercialisation. The University of Latvia received close to EUR 1.6 million in EU contributions spread across three joint projects led by the Israel Institute of Technology (European Commission, 2017). The first of these projects, "Smart Phone for Disease Detection from Exhaled Breath" (SNIFFPHONE), ran from 2015 to February 2019. It integrated heterogeneous micro and nanotechnologies into a smart device that attaches to a mobile phone and analyses disease markers from exhaled breath. The data are then transmitted to a cloud platform for evaluation and a clinical report is sent to the designated receiver (e.g. a specialist) in the event of a positive test result. SNIFFPHONE received the 2018 Innovation Award from the European Commission. The second project, A-Patch, or the "Autonomous Patch for Real-Time Detection of Infectious Disease", applies the science of volatile organic compounds to the analysis of skin data. The technology builds upon a wearable, equipped with an intelligent hybrid sensor array. VOGAS, the third project, runs until December 2021 and aims to develop a new breath analysing device to be used as a non-invasive gastric cancer screening tool.

Repeated involvement in high-profile international research projects suggests that Latvia has established itself as a trusted partner with regard to the testing of medical innovations. The Latvian government should build upon this success by formally integrating industry partnerships and device testing into the public health care system. For example, the National Health Service (NHS) in the United Kingdom introduced a Test Beds Programme in 2016 to allow for the testing of new digital devices and new forms of health service delivery in specific hospitals and for particular groups of patients. Successful innovations can then be scaled up to the entire health system. Several learning handbooks, for example on how to set up data sharing and information governance arrangements, are available and could help Latvia design a similar system (Paunov and Planes-Satorra, 2019).

Latvia should further foster the judicious use of real-world healthcare data to inform biomedical research and evaluation. A "learning healthcare system" based on electronic health records and other routinely collected data holds large promises for making medical research, including with regard to pharmaceuticals, more effective and efficient (e.g. Eichler et al., 2019; OECD, 2019p). However, Latvia stands out from other OECD countries in terms of the absence of national standards for clinical terminology within electronic clinical records and the lack of a national plan or policy to extract data from electronic clinical records systems (e.g. to facilitate clinical trials or monitor patient safety). There is currently also no process to evaluate the usability of electronic health records for dataset creation and healthcare data are mostly not used for research (Oderkirk, 2017).

The testing of medical innovations aside, significant dynamics are also apparent in the area of genomics-based precision medicine and biotechnology. Continuous improvements in digital technologies, including data storage capacities and algorithmic capabilities, have significantly enhanced the feasibility of genetic sequencing. This progress has re-awakened interest in the analysis of genome data and shifted the focus in medical research towards big data and artificial intelligence (OECD, 2020c).

In Latvia, a first physical biobank, the Genome Database of the Latvian Population (LGDB), was established in 2006, legally supported by the Human Genome Research Act of 2004 (Rovite et al., 2018). Since then, several large multinationals, including the Chinese genome sequencing company BGI, Microsoft and Roche, have begun investing in Latvian genomics. For example, in September 2017 Microsoft established LUMIC at the University of Latvia (UL), the first Microsoft Innovation Centre (MIC) of its kind in the Baltics and Eastern Europe. LUMIC focuses on the education of young IT professionals and cloud-based solutions for interdisciplinary IT projects involving students, scientists, industry and government. Genomics-based cancer research is one of the first big data applications to use the new infrastructure. The project is supported through the LIDA initiative Support for Commercialization of Research Results (Vaivare, 2018b).

The push towards digitally enabled genomics in Latvia is partly the result of strong political commitment. In 2017, Latvia signed a Memorandum of Understanding with the Chinese genome sequencing company BGI to promote the creation of the Latvia-Biolake-BGI Life Science and Technology Centre. In November 2019, MGI, a subsidiary of the BGI Group, which produces DNA sequencing instruments, opened the China-Europe Life Health Innovation Centre and a R&D and manufacturing facility in Riga. The same day, BGI Research and MGI announced in Latvia the 10 Million Single-Cell Transcription Project (scT10M), a collaboration with scientists around the world, aiming at sequencing and analysing 10 million cells in an effort to build a comprehensive single-cell transcriptome map to be shared with the scientific community (MGI, 2019).

In May 2019, the Minister of Economics and the Minister of Health jointly launched a conference on precision medicine, with a clear focus on big data analytics and ICTs in health. The conference also addressed the national system of precision medicine in countries such as Sweden, a possible framework for precision medicine research in Latvia and the ethical challenges of using big data in medicine. The MoE is currently developing a common strategy for the biomedicine ecosystem covering the 2021-2027 planning period together with relevant stakeholders from the public sector, industry and academia.

To leverage these dynamics, Latvia should strengthen research in genetics (including clinical) and health informatics. The current number of publications (2014-18) does not suggest research specialisation in these fields and only a small number of publications featured among the 10% most cited publications. Building excellence in these fields requires forming and attracting skills, and the LUMIC innovation centre can be a critical enabler in this regard. LU also offers a doctoral school in translational medicine, partly in co-operation with Rīga Stradiņš University (RSU). However, the faculty of computing currently does not form part of the programme and no specialisation is available in health informatics at LU. In addition, while the RSU has established a bioinformatics research group, the master's programme currently offered in biomedicine is only available in Latvian, severely restricting the attraction of foreign talent. To foster the biomedicine ecosystem and leverage investment by large multinationals, Latvia should further enhance the offer of academic courses at the overlap between medical and computer sciences.

Latvia should broaden the scope of innovation policies for the biomedical ecosystem

Latvia should concentrate more resources in the area of digital health to support the commercialisation of private sector health innovations. Between 2014 and 2018, only 2.5% of all Smart Specialisation spending on biomedicine was devoted to the commercialisation of research results (MoES, 2020). Additionally, funding channelled through competence centres is focused predominantly on pharmaceuticals, cosmetics or nutrition. While private sector e-health solutions, and in particular software, are promoted through the Riga IT Demo Centre (established by the Latvian IT Cluster in 2012), the main focus of the centre seems to be the domestic market. That Latvian health care solutions can also have international appeal is illustrated by the start-up Anatomy Next. The firm developed a Software-as-a-Service (SaaS) solution relying on augmented reality and interactive 3D anatomical models to enhance the spatial awareness of medical students with regard to the human anatomy. The solution won the 2017 Technological Innovation of the Year Award of the Swedish Trade and Investment Council and received EUR 50 000 funding through the H2020 framework's SME instrument.

To foster more innovative firms like Anatomy Next, the government could also provide more support to SMEs and start-ups that apply for H2020 funding. While some support seems to be available for the early stages of the process, many start-ups rely on expensive foreign consultancy firms to manage the

application in later stages. To promote the identification of additional niches of excellence and respond swiftly to newly arising market opportunities (e.g. vaccines, diagnostics or medical technologies in the context of the COVID-19 crisis), support should not be limited to particular fields. However, firms in specific sectors such as health informatics could be targeted through cluster initiatives.

The government should further consider adjacent sectors as part of the biomedicine ecosystem. For example, significant export potential for health services was recognised during an initial evaluation of potential Smart Specialisation areas (MoES, 2013b). Thus, between 2005 and 2015, Latvia came close to developing an RCA in exports of human health activities (Figure 6.13); and while firms in the sector spent only 0.07% of total value added on R&D, the distance to the OECD average (0.13%) was lower than in many other sectors (Figure 6.15).

Providing a testbed for healthcare innovations, as suggested above, could be a promising way for Latvia not only to enhance the moderate quality of its public health care system (OECD, 2019a), but also to establish itself internationally as an innovative provider of health services. For example, Latvia could extend its participation in the ProVaHealth network. ProVaHealth is one of 39 approved Interreg Baltic Sea Region projects, and aims to establish the region as a single test site for the development of new health care products and services. Currently, Latvia's participation is limited to well-being, with the Latvian Resorts Association as the only participant. However, other companies, research institutes or universities could enter the project to benefit from the project's Living Labs, providing a real-life testing ground for innovative healthcare solutions.

Synergies could also be created with regard to the national e-health initiative, which since 2018 has made use of the national e-health portal mandatory for prescription and sick leave services. Despite this significant progress, the launch of the third phase of the strategy, an extension of the system, is advancing relatively slowly (MoH, 2019). To improve population health and reduce the significant disparities that still exist in terms of access and outcomes in the public health care system, the government should advance the e-health agenda, including with regard to health data (see above) and telemedicine. Areas such as prevention, primary care, home care or community-based services seem especially promising areas for applications that could reduce the current high reliance on hospital treatments (OECD, 2019l).

Box 6.9. Policy recommendations: Biomedicine

- Build upon research excellence in translational medicine by developing industry partnerships and test beds for new medical devices in the public health care system.
- Leverage private investments in digital research infrastructure by strengthening academic outputs in the area of health informatics and genomics.
- Enhance spending in the field of digital health and commercialisation of digital health products, including software. Support start-ups and SMEs in applications for H2020 funding to promote clusters of excellence.
- Leverage national e-health initiatives and existing collaborations with other countries (e.g. ProVaHealth) to test and promote innovative health care services and enhance the quality of the public health care system.

Improving targeting of innovation policies

Increasing the rate of discovery and development of new and improved materials is key to enhancing product development and facilitating mass customisation based on emerging technologies such as 3D printing. Acceleration of the discovery and development of materials has been enabled by advances along multiple fronts, including data analytics, the capabilities of scientific instrumentation, high-performance computing and predictive computational methods applied to material structure and properties (OECD, 2017b). Latvia's RIS3 considers Smart Materials a core area for research specialisation.

In addition to new materials, such as implant materials, composite materials, glass fibre and glass-based materials, or thin layers and coatings, the Smart Specialisation area also covers a wide range of manufacturing activities related to technology and engineering. These include, among others, equipment and control systems for manufacturing activities, medical engineering and biotechnology. These different activities are reflected in several manufacturing industries, such as fabricated metal products, non-metallic mineral products, machinery and chemical products.

Smart materials and engineering can rely on a robust research environment and successful industry performance

Many of the above sectors have grown in importance in recent years. The contribution to total manufacturing value added of fabricated metal products, such as those related to engineering and coatings, grew from 6% in 2010 to 9% in 2017. Over the same period, the contribution of other non-metallic mineral products, including glass. fibre-based materials, grew from 6% to 7.4%. Rubber and plastic products, which are not listed under the relevant sectors for smart materials in the Latvian strategy, but link to new packaging materials such as bioplastics and composite materials, also increased, from 2.2% to 2.5%. The contribution of machinery and equipment (not otherwise considered), related to technology and engineering, increased from 2.2% to 3.3%. However, the contribution of chemical products diminished significantly from 4.5% to 2.5% (Figure 6.12).

Export performance has also improved significantly in recent years. Manufacturing activities related to motor vehicles, electrical equipment or machinery has contributed considerably to the increasing share of medium-high and high technology goods in exports (Figure 6.17). Although Latvia had no RCA in these industries as of 2015, the country developed an RCA in non-metallic mineral products over the years 2010-15, and came close to an RCA for fabricated metal products (Figure 6.13).

Business R&D as a share of value added in non-metallic mineral products (1.1%) was below the OECD average (2.5%). However, the distance from the OECD average, both in absolute and relative terms, was significantly lower than in most other manufacturing sectors. Investments in research were also relatively high for electrical equipment (5.3% compared to 6.8%). Distances from the OECD average for R&D intensity were larger for other manufacturing industries, including chemicals (1.8% compared to an OECD average of 5.4%), rubber and plastics (0.3% compared to 4.1%), and machinery and equipment (0.3% compared to 6.8%) (Figure 6.15).

R&D activities in the area of smart materials and engineering were also reflected in several patent applications between 2012 and 2016 in the fields of (other) special machines, surface technology and coatings, electrical machinery, apparatus and energy, materials in metallurgy and chemical engineering. The number of patent applications (including fractional counts) in the above fields increased from 10.0 (9% of all Latvian applications) in 2007-11 to 26.1 (20%) in 2012-16.

Scientific publications confirm Latvia's strong specialisations in engineering and materials. While the number of Latvian publications in 2014-18 was highest in electrical and electronic engineering, the strongest specialisation relative to other countries was found in automotive engineering, industrial and manufacturing engineering, and biomaterials. Furthermore, Latvia contributed more than 10% (the global average) to the top 10% most cited publications in fields such as the mechanics of materials, metals and alloys or mechanical engineering (Figure 6.19).

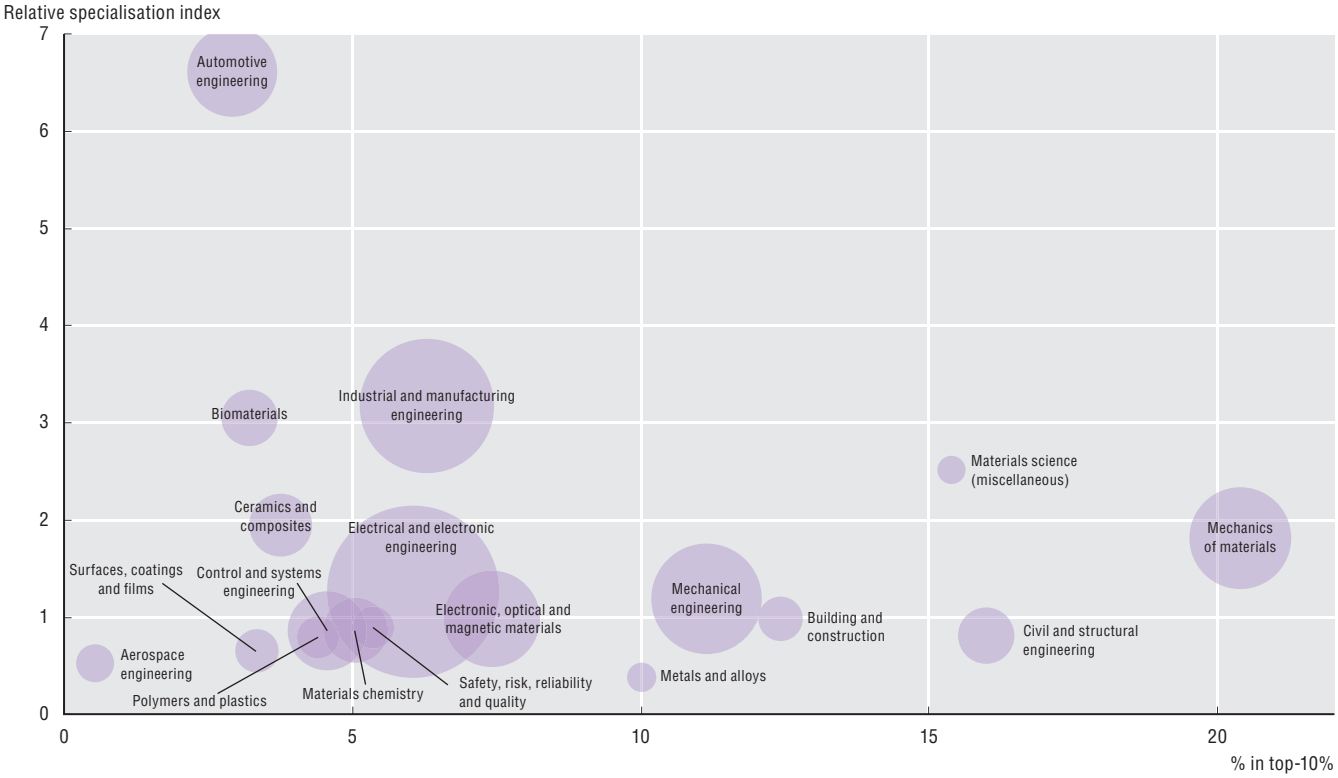
Government support for material sciences needs to be better targeted and should be complemented by general support mechanisms for innovative firms

Research in the smart materials specialisation area has been fuelled by significant public funding through the Smart Specialisation Strategy. The area received the largest share of funds among all Smart Specialisation areas with over EUR 52 million in funding (27.5%) (Table 6.2).

However, allocation of funding was spread too thinly across a large number of research topics. In the best cases (e.g. for fields such as thin layers and coatings or composite materials and polymers), several million euros were allocated to support different stages of maturity, from basic technology research (TRL 1) up to demonstrations in a relevant environment (TRL 6). However, other research topics, such as medical engineering or implant materials, received only EUR 340 000 and EUR 600 000, respectively, focusing on particular stages of technological maturity.

Figure 6.19. Latvia's publications in the top 10% most cited documents on material sciences and engineering

Average, 2014-18



Notes: Size of shapes represents number of publications, ranging from 7 (Materials – miscellaneous) to 281 (Electrical and Electronic Engineering). Number of publications are totalled over the years 2014-18. See Figure 6.18 for more details.

Source: OECD calculations based on Elsevier, Scopus Custom Data, Version 5.2019.

To increase effectiveness of spending, Latvia should concentrate funding on a smaller number of selected ecosystems that allow for close linkages between materials discovery and product development. The development of a more comprehensive material innovation ecosystem, involving research universities and manufacturers, is key to reducing the lag between these stages. Digital technologies, including computational material science and digital twins, are crucial enablers in this regard, as they help to connect the different stages of the materials production life cycle (OECD, 2017c). For example, Integrated Computational Materials Engineering (ICME) uses data science, computational modelling and simulation to link the development of materials to the certification of properties and product deployment more efficiently. The Laboratory of Magnetic Soft Materials at the University of Latvia, in co-operation with the Institute of Experimental Physics SAS (the Slovak Republic), Cordouan Technologies and LCPO (France), is currently involved in an ICME project focusing on the properties and applications of magnetic filaments in areas such as energetics, textiles and medicine. The project is financed through M-ERA.NET (see below).

A positive example of increasing linkages between research and manufacturers is the Excellence Centre of Advanced Material Research and Technology Transfer (CAMART). Originally established in 2001, CAMART is run by the Institute of Solid State Physics (ISSP) of the University of Latvia in co-operation with two Swedish partners, the KTH Royal Institute of Technology and Acreo Swedish ICT. The Centre receives funding from the Horizon 2020 framework (EUR 15 million) and ESIF funds (EUR 16.3 million). In 2018, CAMART launched Materize, a brand and platform to foster the transfer of new materials and technology to commercial products. Materize provides services ranging from proof-of-concept in the laboratory environment to prototyping and small-scale production in industrial test beds provided by partners.

Latvia should seek to actively enhance linkages between materials discovery and product development by making funding available for different technological maturity levels (TRL 1-6) within a selected materials ecosystem, from basic technology research to technology demonstration and the commercialisation of research results. The Baltic Biomaterials Centre of Excellence (BBCE) is an example of an ecosystem where such an approach is already underway. Latvia could also focus export support on firms that have previously benefited from publicly funded R&D (e.g. through competence centres).

For research fields with less developed innovation ecosystems, Latvia should focus on more general support mechanisms that can help to improve linkages between firms and public research institutes or universities. In particular, Latvia should strengthen its Technology Transfer Programme and foster incubators at universities. At present, there also seems to be no overarching strategy to promote co-operation between start-ups and research facilities, with many start-ups reporting difficulties identifying suitable research partners (MoE, 2018c). With the launch of the website StartupLatvia.eu, the Latvian government has recently introduced a centralised one-stop shop for start-ups. However, relevant information on technology transfer offices and opportunities for research collaboration are not currently available.

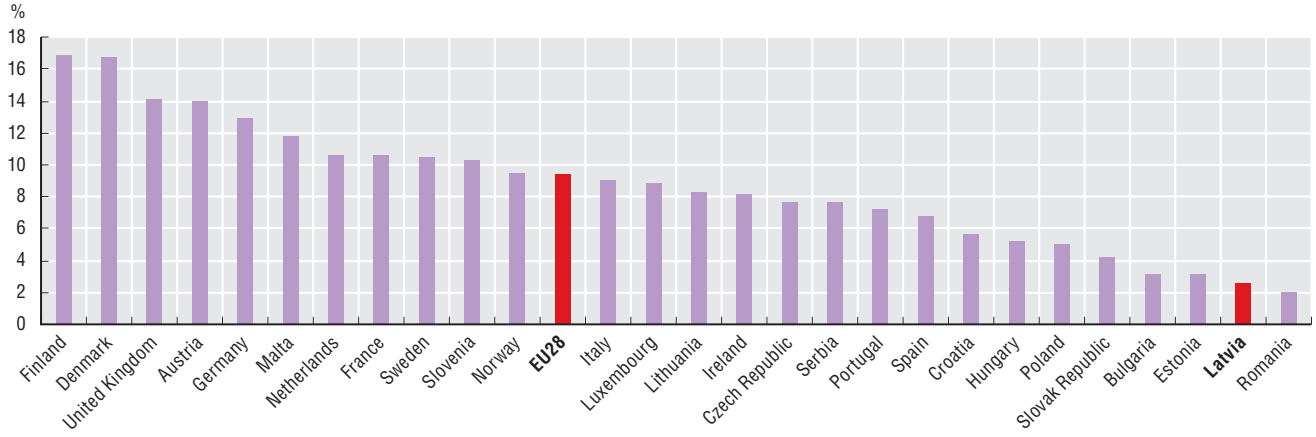
The Latvian government should also provide more support for excellence-based innovation calls such as Horizon 2020. Through its national contact points (e.g. SEDA), the government could provide targeted training workshops for applicants (e.g. in co-operation with universities, cluster initiatives or competence centres) or more actively approach innovative private sector stakeholders. Indeed, a collaboration involving several institutions, including SEDA and the MoEs as well as external experts, has helped to increase significantly the success rate of Latvian research proposals to M-ERA.NET, an EU-funded network issuing annual calls for transnational R&D projects on materials sciences. In particular, the percentage of proposals that were accepted for funding increased from 5% in 2012-14 to almost 20% in 2017-18.

Latvia should foster uptake of advanced manufacturing technologies in downstream sectors

The Latvian government should foster wider uptake of digital manufacturing technologies in downstream sectors. For example, Latvian manufacturing firms are lagging behind in the use of 3D printers (Figure 6.20).

Figure 6.20. Business use of 3D printers in manufacturing in Latvia and selected OECD countries, 2018

As a percentage of all manufacturing firms



Source: Eurostat (2020a), *ICT Usage in Enterprises – E-business (isoc_eb)* (database), *https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/database*.

Latvian stakeholders are beginning to actively promote the uptake of digital production technologies in core manufacturing industries. In 2016, the industry association for firms in mechanical engineering and metalworking industries (MASOC) engaged in the cross-country co-operation programme Empower Metalworkers for Smart Factories of the Future (4CHANGE). The project, which was co-funded by the "EU Erasmus+" programme and ran until November 2019 with a budget of about EUR 1.2 million,

aimed to enhance vocational education and training (VET) programmes, with a focus on the use of computer numerically controlled (CNC) machines. However, as of 2018, about half of firms in mechanical engineering and metalworking industries still perceived themselves as low digitally intensive (Grinfelds, 2018).

In order to foster and extend similar projects to other industries, the government, together with several competence centres and the German-Baltic Chamber of Commerce (AHK), has recently signed a Memorandum of Understanding on Development and Implementation of the Platform Industry 4.0 (Box 6.10).

Box 6.10. Platform Industry 4.0

To increase the use of digital technologies in the manufacturing sector, Latvia is developing an Industry 4.0 Implementation Package which aims to improve links between Latvian manufacturing firms and enterprises developing smart technologies. In February 2019, a Memorandum of Understanding on Development and Implementation of the Platform Industry 4.0 was signed by the Ministry of the Economy, the Ministry of Environmental Protection, eight competence centres and the German-Baltic Chamber of Commerce (AHK), which includes companies such as SAP and Bosch. Platform Industry 4.0 aims in particular at strengthening co-operation and co-ordination between stakeholders, advising Latvian firms with regard to new technologies for the manufacturing sector and designing policies to promote digital technologies. The Ministry of Economy is currently developing a strategy to implement the Memorandum.

The government aims to leverage DIH as a physical platform for the implementation of Platform Industry 4.0. These hubs would serve as a one-stop shop where firms and, in particular, SMEs, as well as public sector organisations, could access services related to testing, attracting investors, skills and training, networking and the innovation ecosystem. According to the government, Platform Industry 4.0 will be established formally through the Digital Europe Programme (2021-2027), which proposes to make available EUR 9.2 billion for areas such as supercomputing, artificial intelligence, and the build-up and strengthening of the European DIH network.

For the implementation of the Latvian Platform Industry 4.0, which is currently still in the planning phase, Latvia should consider some of the approaches used by other countries to foster the uptake of digital tools, in particular among SMEs. For example, the SME 4.0 Competence Centres in Germany offer demonstrations of new technologies and industry applications to SMEs. These demonstrations are often performed at universities and are tailored to specific sectors. In Denmark, the MADE programme organises visits to industry leaders willing to share their experience with evolving state-of-the-art solutions (Paunov and Planes-Satorra, 2019). Latvia could also consider opportunities beyond the Digital Innovations Hubs (of which only three are currently active) to promote interactions with new technologies among SMEs. For example, Latvian clusters, potentially in co-operation with clusters in other countries, could organise visits for SMEs to local or international industry leaders. Additionally, competence centres could offer targeted demonstrations of relevant new technologies for SMEs.

The programme Brasil Mais Productivo provides another example that could help foster Industry 4.0 in Latvia. The programme offers targeted consultancy services to help generate process innovation in small and medium-size manufacturing firms. The programme involves about 120 hours of technical training on lean manufacturing, energy efficiency practices and digitalisation of the production process. The focus on consultancy limits the cost of the programme. Additionally, companies are required to pay a share of the costs, which helps to ensure active participation. A specific credit scheme helps entrepreneurs with limited funds to overcome the financial burden of the programme. In the absence of an institutional structure to provide such consultancy services across Latvian regions, specialised courses on lean manufacturing and the use of advanced technologies could also be incorporated into the business training courses provided by LIDA within the framework of the Innovation Motivation Programme.

Box 6.11. Policy recommendations: Smart materials and engineering

- Target funding from the Smart Specialisation Strategy towards a smaller number of selected ecosystems allowing for closer links between materials discovery and application. Support innovation in selected ecosystems along the full innovation cycle, from early stage research to marketing and internationalisation.
- Support excellence in other research fields through broader innovation support mechanisms, including technology transfer programmes, university incubators and training for H2020 applications (e.g. by SEDA).
- Finalise and implement the Industry 4.0 Implementation Package to foster digital uptake in manufacturing firms, in particular SMEs. Leverage clusters and competence centres to disseminate knowledge about advanced manufacturing solutions and promote consultancy services and training (e.g. through LIDA).

Smart Energy technologies and Smart City solutions

The Latvian Smart Specialisation Strategy considers smart energy and ICTs as sectors with significant horizontal impact on transformation in other manufacturing sectors. The Smart Energy specialisation area, in particular, underscores the role of improved energy efficiency and clean technologies for enhanced productivity and environmental sustainability across economic sectors (MoES, 2015).

Smart Energy is highly dynamic in Latvia but uptake of energy saving technologies remains low

Sectors producing Smart Energy technologies are growing. In particular, the share of electrical equipment in total manufacturing rose from 1.5% in 2010 to 3.3% in 2017, while the contribution of machinery and equipment increased from 2.2% to 3.3%. Other related industries, such as manufacturing of motor vehicles and trailers, also increased in importance (1.5% to 2.5%) (Figure 6.12).

All three industries also contributed significantly to an increase in the share of high and medium-high tech goods in total manufacturing exports (Figure 6.17). However, in neither did Latvia reveal a comparative advantage (Figure 6.13).

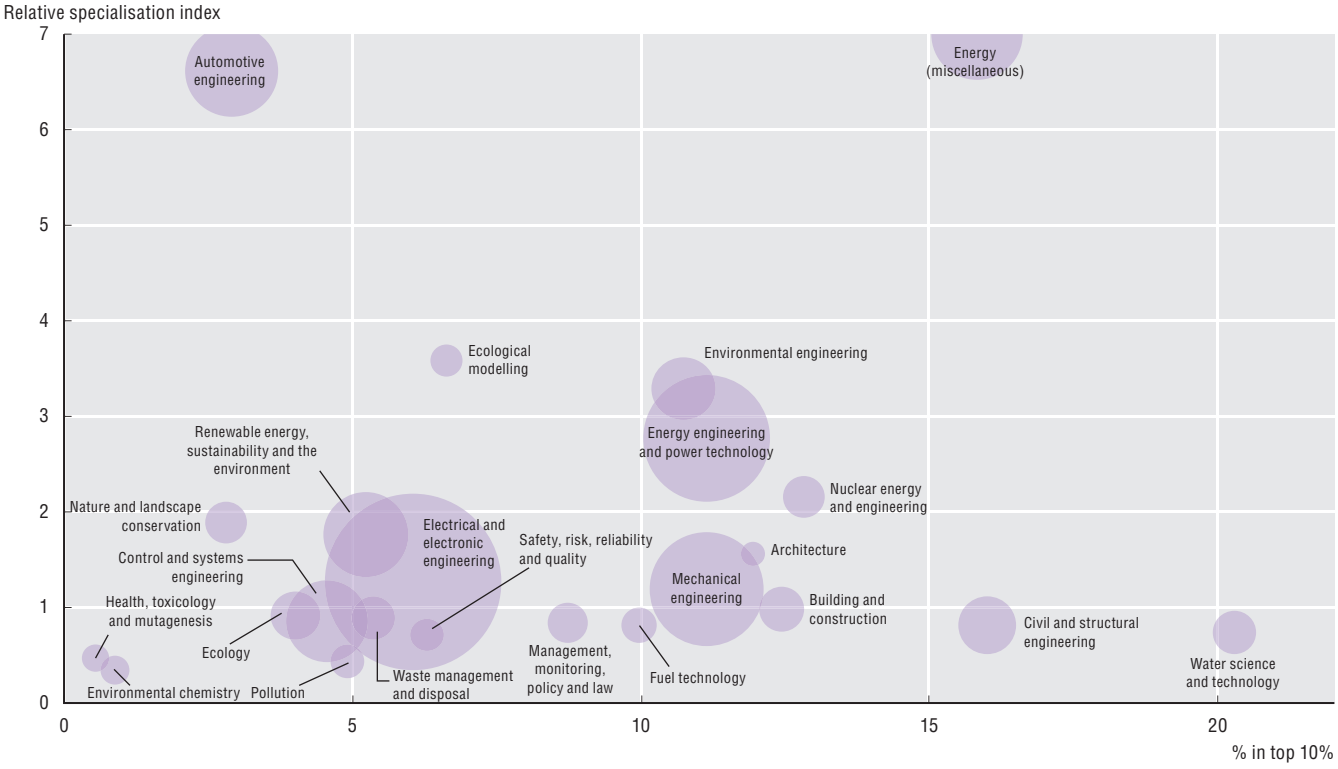
Business R&D on electrical equipment, however, was far higher than in any other manufacturing industry (5.3%), and came relatively close to the OECD average (6.8%) (Figure 6.15). Similarly, the number of patents in electrical machinery and apparatus, transport and environmental technology increased from 2007 to 2016.[8]

The energy and environmental sciences are among the most successful research areas in Latvia. According to the European Eco-Innovation Index, in 2018 academic output in the field of eco-innovation was greater in Latvia than in any other EU country. Publications in related fields of research were published relatively more frequently than in other countries (i.e. compared to the world average), and the share of frequently cited documents was also higher. In particular, over the years 2014-18 around 17.3% of Latvian publications in the field of Energy were among the top 10% most cited publications worldwide (Figure 6.21). In the environmental sciences, research performance was highest for environmental engineering and water science and technology, where 17% of Latvian publications were among the top-10% most cited worldwide. Publications in other related engineering fields, such as civil and structural engineering (16%) or building and construction (13%), were also frequently among the top 10%.

Between 1990 and 2016, Latvia more than doubled energy production, from 1.2 million tonnes of oil-equivalent (Mtoe) to 2.5 Mtoe. Over the same period, net energy imports declined from 7.5 to 2.2 Mtoe, implying significantly lower dependency on foreign suppliers (IEA, 2019a). Biofuels and waste have become key sources of energy supply – as of 2018, Latvia had the third highest share of energy from renewables in gross final energy consumption (40.3%) among all EU countries, after Finland (41.2%) and Sweden (54.6%) (Eurostat, 2020b).

Figure 6.21. Latvia's publications in the top 10% most cited documents on smart energy

Average, 2014-18

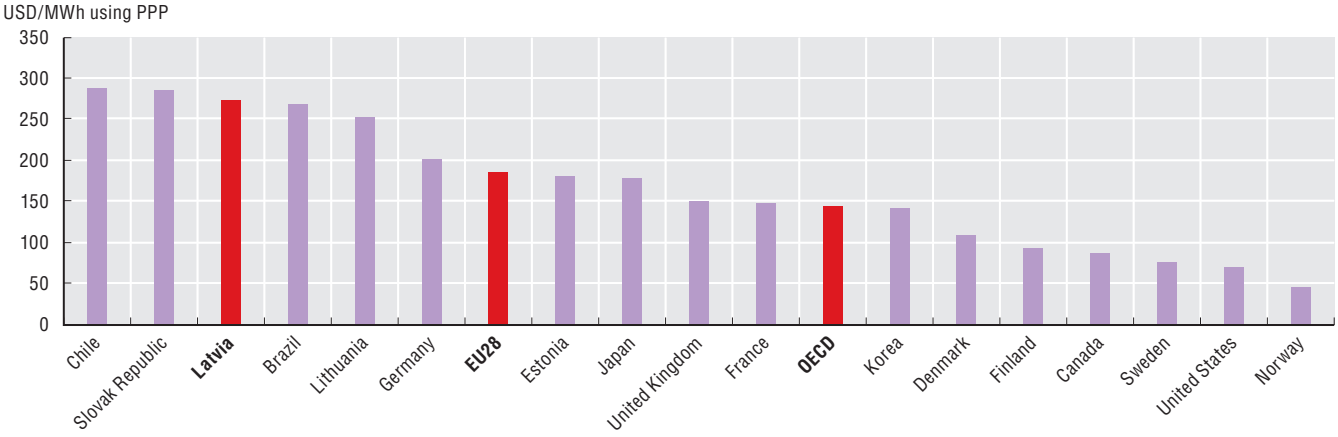


Notes: The size of shapes represents the number of publications, ranging from 5 (Architecture) to 281 (Electrical and Electronic Engineering). The number of publications is totalled over the years 2014-18. See Figure 6.18 for more details.

Source: OECD calculations based on Elsevier, Scopus Custom Data, Version 5.2019.

However, while Latvia is on track to achieve its 2020 energy efficiency target, energy consumption is on the rise, driven by the transport and the residential sectors. Furthermore, energy production from biomass remains highly inefficient and, together with growing urban transport and low energy efficiency in housing, threatens the achievement of Latvia's 2030 energy efficiency targets (European Commission, 2020; OECD, 2019a). The country also still needs to improve sustainability in waste management, as the recycling rate in municipalities remains low. Additionally, Latvia has some of the highest industrial electricity prices in the world (Figure 6.22), which are regarded by many firms as a major challenge to competitiveness (e.g. Grinfelds, 2018).

Figure 6.22. Industrial electricity prices in Latvia and selected OECD countries, 2017



Note: MWh = megawatt-hour.

Source: IEA (2019b), *World Energy Prices*, *http://data.iea.org/payment/products/121-world-energy-prices-2019-edition.aspx*.

Commercialisation of innovative clean technologies needs stronger policy support

With about EUR 34 million in funding in 2014-18, Smart Energy accounted for less than one-fifth of total support to Smart Specialisation. Most of R&D funding has been invested in developing technologies and solutions for improving energy efficiency in buildings and industry (30%) and energy management, including smart grids (29%). Alternative fuels, including electro mobility, received 22%. Over one-third of the total R&D funding for Smart Energy was provided through the Horizon 2020 framework (36%), a share significantly higher than in all other RIS3 areas, where the share of H2020 ranged from 5% (Biomedicine) to 23% (ICT) (Table 6.2).

The largest projects funded under this scheme are SUNShINE and SUNShINE Accelerate, each of which benefits from EU contributions of close to EUR 1.3 million. The projects target the renovation of residential buildings, and are co-ordinated by Riga Technical University. While they promote energy efficiency in Latvian housing and foster demand for energy services, there are no conditions regarding the technologies used by projects, implying that the effects on innovation remain uncertain.

Digital innovation, in particular, can be a crucial enabler of energy savings. According to the International Energy Agency (IEA), the use of digital technologies such as smart thermostats and smart lighting in buildings has the potential to create global energy savings of around 65 PWh up to 2040 – the total final energy consumption of OECD partner economies in 2015 (IEA, 2017). Similarly, the use of digital technologies in transport (e.g. smart charging of electric vehicles, shared and automated mobility) and industry (e.g. additive manufacturing, digital twins) could unlock significant energy savings and emission reductions. Latvia should therefore specifically foster *smart* energy innovations, including the application of digital technologies in buildings, transportation and industry, to help achieve energy and cost savings.

Two H2020 projects that highlight successful research activity in this regard are MORE-CONNECT and RealValue. MORE-CONNECT focused on the design and piloting of modular, prefabricated renovation elements that communicate through wireless sensors and control components for performance diagnostics and control. The project represented a collaboration between RTU (EUR 330 450), the Latvian Wood Construction Cluster (EUR 56 875) and the Zemgales Technological Centre (EUR 78 925) along with 15 other participants from seven countries, and was completed in May 2019. RealValue demonstrated the potential of Smart Electric Thermal Storage (SETS) as a replacement for existing electric thermal storage heaters and water tanks. The project involved RTU (EUR 632 318) along with 11 partners from Finland, Germany, Ireland and the United Kingdom, and was completed in May 2018. SETS devices were deployed together with smart plugs, sensors and smart meters in 1 250 homes in Germany, Ireland and Latvia. A gateway connects the devices to a cloud optimisation engine, which links to the electricity grid in each country to calculate and implement optimised charging schedules. RTU was also involved in the energy system modelling exercise, which helped demonstrate the potential of technical and commercial deployment in millions of homes across representative EU regions.

Innovation in smart energetics is also picking up in the private sector, where a number of start-ups with a focus on digital technologies have been emerging. For example, Citintelly, founded in 2016, has developed a multifunctional cloud-based Street Lighting Central Management System (CMS), including sensors and controllers, and has to date implemented projects in Israel, Latvia and Malta. Meanwhile, Route4Gas is developing software solutions for better gas routing in the European natural gas market. Additionally, Marine Digital, one of the first international start-ups settling in Latvia in the context of the country's start-up visa programme is offering an automated port and bulk-terminal management system (see the first section of this chapter).

To support start-up dynamics and private sector innovation, the government should increase funding for research commercialisation and competence centres. Smart Energy is the Smart Specialisation area with the least spending in these areas, which fall under the responsibility of the MoE. Together, they account for only 12% of total spending (EUR 4 million) in the Smart Energy specialisation area, compared to 22% in biomedicine and around 39-43% in other areas (EUR 10-20 million) (Table 6.2).

Latvia should specifically target eco-innovation, in order to better exploit synergies between Smart Specialisation and measures that support cleaner production, waste prevention or bioenergy (OECD, 2019m). While eco-innovation cuts across several Smart Specialisation areas, including Smart Energy,

Bioeconomy and Smart Materials, it is not currently the focus of any one area. Accordingly, environmental innovators are represented in four different clusters, namely: the Latvian Electronics and Electrical Engineering Cluster, the CLEANTECH Cluster, the Green and Smart Technology Cluster, and the Smart City Cluster. Stakeholder interviews with cluster representatives seem to confirm that some firms in these clusters have faced significant difficulties in locating appropriate support mechanisms within the Smart Specialisation framework.

The government could, for example, replace or revive the Green Industry Innovation programme, which provided pre-incubation and incubation services to start-ups engaging in the development and commercialisation of environmental technology. The initiative, which started in 2014, was run by the MoE as part of the Norwegian Financial Instrument Programme. As of April 2017, 152 teams had received pre-incubation advice from a specialised green technology incubator and 23 project implementers had benefited from co-funding totalling EUR 2.4 million (MoES, 2018). The programme is currently inactive in Latvia due to a lack of funding.

Smart Energy and environmental technologies stand to benefit substantially from Smart City initiatives

One promising concept that provides significant potential for the Smart Energy specialisation area in the context of digital transformation is Smart Cities. Smart cities are closely linked to the emergence of new digital technologies in areas such as energy efficient buildings, smart grids, smart mobility solutions, and sustainable waste and water treatment solutions.

For example, the "Riga Smart City Sustainable Energy Action Plan for 2014-2020" (SEAP), through which the city of Riga has committed to reducing CO_2 emissions by at least 20%, is based on a 20% increase in energy efficiency and an increase in the share of renewable energy in total consumed energy to 20%. The integration of innovative ICTs into energy and transportation systems is a core component of the programme. SEAP was developed within the EU Seventh Framework programme "Strategies towards Energy Performance and Urban Planning" (STEP-Up) in collaboration with municipalities in Belgium and Sweden and the United Kingdom.

One of the actions foreseen under the programme is an upgrade of the city's lighting system to programmable LED lamps. However, progress has been rather slow since the programme's launch in 2012, with "smart" control of LED streetlights currently restricted to a limited number of neighbourhoods. This includes Maras Park, which in 2017 was equipped with smart lighting technology by the Latvian start-up Citintelly. In 2019, an agreement was signed worth over EUR 4.7 million for three new projects to advance the implementation of smart lighting solutions in Riga. The projects involve remote control systems with presence radar detection for light and traffic control.

Further investments are also required in the transport system. Most transport-related investments in the past have focused on the road network, with cars still accounting for the vast majority of passenger travel in Latvia. Currently there is no integrated public transport system linking Riga to neighbouring municipalities, implying that services such as route planning, pricing and ticketing are separated across several providers and municipalities (OECD, 2019m). Developing an integrated public transport system with a metropolitan transport authority, such as those in Madrid, Prague or Warsaw, could make travel easier and more affordable, and allow for the digital integration of ticketing and route planning systems. Fostering alternative shared and active mobility solutions, such as bicycles, electronic cars or scooters, could further incentivise commuters to leave their car at home and make transport more inclusive and sustainable.

Among smaller municipalities, the city of Jelgava has been one of the earliest adopters of a Smart City vision. Since 2016, critical infrastructure in the city has been monitored by a Joint Municipality Operative Information Centre (JMOIC), which includes real-time monitoring of traffic flow data, traffic optimisation through smart traffic lighting, and automated monitoring of meteorological stations and flood protection gates, as well as smart energy management solutions for district heating. Additionally, citizens were provided with e-cards (NFC technology) that can be used to pay for public transportation and receive social benefits. In 2017, the investment research department of the *Financial Times* ranked Jelgava 6th among European micro-cities in the category "connectivity" (Strods, 2017).

The Smart City concept is gaining traction across Latvia following the identification of Smart Cities as a core value chain for the revised version of the Smart Specialisation Strategy. The MoE is currently defining the details of the value chain, in consultation with public, private and academic stakeholders, as well as in co-ordination with the ministries of Transport and Environmental Protection and Regional Development. MoE representatives and other stakeholders have also engaged with international peers to learn more about the realisation of Smart City concepts in countries such as the Netherlands or at the Smart City Expo in Barcelona.

One indication of increasing dynamism is the initiative VEFRESH, an open innovation movement launched in 2019 by technology companies, real estate developers and the Riga municipality. The movement aims to transform Riga's VEF district – which hosts a large share of Latvia's IT sector and accounts for over 40% of the country's IT exports – into a testbed for smart city solutions. The national government can play an enabling role in support of innovative solution delivery, capacity building and upscaling in the context of smart cities (OECD, 2020i), and has signalled its direct support for Smart City developments in the VEF neighbourhood through a recent MoU signed between the MoE and Riga City Council.

The town of Cesis has also begun to develop a digital strategy and is organising seminars and workshops for business people on variety of data tools, including artificial intelligence. The Cesis district municipality has received support from the private sector-driven initiative Valsts#196, which provides a platform for dialogue between municipalities and providers of technological solutions. The Latvian IT Cluster is one of the co-founders of the initiative.

Latvia should further integrate the smart city concept into national and regional development strategies to leverage complementarities and enhance co-ordination with other policies which aim to increase quality of life and investment opportunities across the country, including in small municipalities. The existence of a national framework for smart city solutions is important as it can empower and guide local governments to identify their main needs and opportunities. The Canadian government, among others, is actively fostering smart city solutions in smaller municipalities through the Smart Cities Challenge. This competition, which is open to municipalities, regional governments and indigenous communities, encourages participants to adopt innovative technologies to improve the lives of their residents. Four initiatives will be selected and receive federal funding. An important requirement is that projects are scalable and replicable.

An increasing number of good practices worldwide could inspire smart city policies in Latvia. For example, Finland's Six City Strategy (6Aika), launched in 2014, includes the development of an open innovation platform where stakeholders in the six largest cities can share smart solutions. Participating stakeholders can freely experiment with innovative solutions in all six cities. In France, the public investment bank has created a special fund (*Ville de Demain*) to provide financial support to start-ups offering smart city solutions. In addition to financial support, Japan grants regulatory exceptions to cities prepared to implement smart city projects. These and other examples are discussed in (OECD, 2020i; 2019n), which take stock of a decade of experimentation, uptake and proliferation of smart city initiatives across the globe (Box 6.12).

Latvia should make more extensive and strategic use of public procurement to promote innovation among regions and municipalities.[9] The OECD Framework to Promote the Strategic Use of Public Procurement for Innovation discusses several action areas that could guide Latvia in efforts to strengthen procurement for innovation (OECD, 2017d). Removing financial and regulatory barriers to the participation of SMEs in public procurement bids will also be crucial (see Chapter 4). Many countries have developed integrated procurement plans with explicit targets for innovative projects at the municipality level. In Sweden, for example, some municipalities have incorporated innovation targets into procurement procedures, while VINNOVA, the Swedish Innovation Agency, provides support to contracting authorities that wish to procure innovation in the form of financing possibilities (OECD, 2017d). The Latvian Ministry of Finance is currently analysing the potential for greater usage of public-private partnerships, which have been used successfully in other countries to finance smart city projects (Deloitte, 2018).

Box 6.12. Enhancing the contribution of digitalisation to smart cities of the future

Digital transformation brings opportunities for ground-breaking innovations in urban design, policy making and infrastructure. Cities are already tapping this potential, often with the close involvement of the private sector. Municipalities are using data and digital technology to help tackle climate change, foster inclusive growth or improve administrative processes by searching for efficiencies, cutting red tape or engaging citizens. Sector-driven technologies have also contributed to new social initiatives, actions to combat climate change and green growth in cities.

A search on Google Trends suggests that worldwide interest in smart cities has increased significantly since 2013, making "smart" the most popular adjective in relation to cities, surpassing others such as sustainable, healthy, liveable, green and resilient. The smart city concept itself is evolving and is still subject to debates. Highlighting the crucial role of citizens' well-being, the OECD has defined smart cities as "initiatives or approaches that effectively leverage digitalisation to boost citizen well-being and deliver more efficient, sustainable and inclusive urban services and environments as part of a collaborative, multi-stakeholder process" (OECD, 2020i). This definition as well as recent OECD discussions stress in particular:

- the need to design, implement and monitor smart city policies, to ensure that the rapid diffusion of new technologies improves well-being for all people
- the enabling role that national governments can and should play to support innovative solution delivery, capacity building and upscaling
- the critical role of a comprehensive, multi-sectoral and flexible framework that helps advance the measurement agenda and is aligned with local and national strategic priorities, and embraces efficiency, effectiveness and sustainability dimensions
- the need for holistic and smart governance, which sometimes requires re-regulation rather than simple de-regulation, leverages public procurement, and employs business and contractual models that able to adapt rapidly to changing urban environments.

The central role of citizens not only as recipients, but also as actors of smart city policies, implies the co-construction of policies throughout the policy cycle. Policy makers, however, still often lack a clear understanding of the challenges, risks and trade-offs of digital innovation in cities. Indeed, digital transformation can either improve the public policy response to other transformative megatrends, such as globalisation, demographic shifts and climate change, or reinforce their destabilising effects. In the absence of an integrated, multi-sectoral and whole-of-government perspective, digital innovations can upend legal and regulatory frameworks that safeguard affordability objectives, consumer protection, taxation, labour contracts or fair competition. They can also jeopardise citizen data, privacy and safety, thus generating trade-offs between data disclosure and the perceived impacts of smart city services.

To ensure that digitalisation does not widen social inequalities or contribute to further citizen discontent and a backlash against public institutions, public and private actions must be evaluated in terms of their value to society, and smart city applications should be well connected with inclusive growth objectives. Investment in human resources, for example through life-long learning, and efforts more generally to ensure that people have the skills they need for future work, including digital literacy, must be implemented in all cities and regions, and should be viewed as an investment and not a cost.

Source: OECD (2020i), *Smart Cities and Inclusive Growth*, *www.oecd.org/cfe/cities/OECD_Policy_Paper_Smart_Cities_and_Inclusive_Growth.pdf*; OECD (2019n), *Enhancing the Contribution of Digitalisation to the Smart Cities of the Future*, *www.oecd.org/cfe/regional-policy/Smart-Cities-FINAL.pdf*.

Latvia should also develop regulatory sandboxes to help overcome the regulatory challenges and uncertainties related to smart city initiatives. The British Office of Gas and Energy Markets (Ofgem) provides an interesting model in this regard. Ofgem has created a one-stop shop for the *energy* sector, offering rapid advice on energy regulation to businesses. When regulatory barriers prevent the launch of a product or service that would benefit consumers, a regulatory sandbox can be granted to permit a trial (Paunov and Planes-Satorra, 2019).

Box 6.13. Policy recommendations: Smart energy

- Target eco-innovation by broadening the scope of the Smart Energy specialisation area to include environmental technologies (e.g. for waste and water treatment).
- Re-allocate Smart Specialisation funds towards research commercialisation and competence centres.
- Re-establish a Green Industry Innovation programme with an adequate level of resources.
- Integrate the smart city concept into regional development policies to promote eco-innovation and increase the quality of life and investment opportunities in all regions.
- Foster smart city solutions through financial support to innovative municipalities, open innovation platforms, smart procurement and regulatory sandboxes.

Improving synergies within RIS3 areas

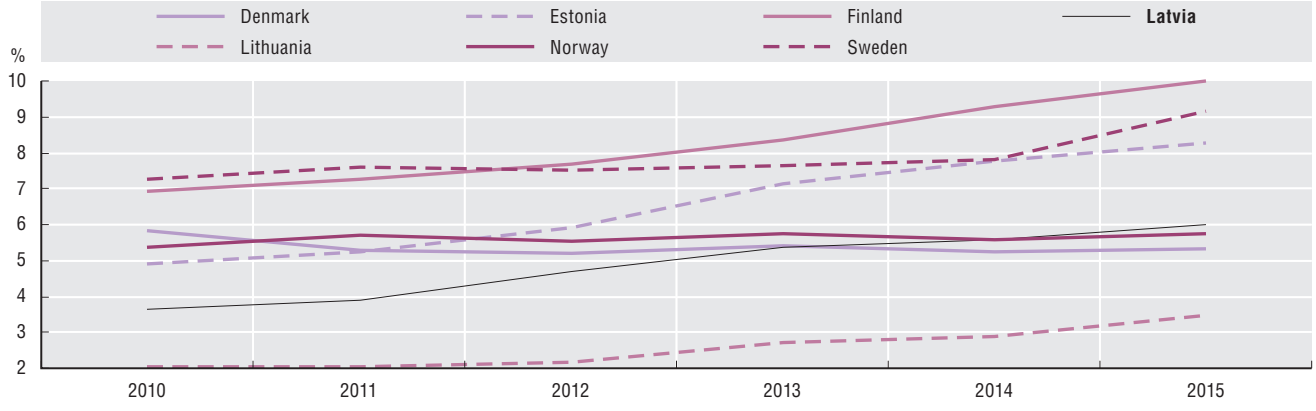
As noted earlier, the Latvian Smart Specialisation Strategy considers smart energy and ICTs as sectors with significant horizontal impact on transformation in other manufacturing sectors (MoES, 2015). This section considers ICT goods and services, including related manufacturing industries such as consumer electronics.

ICT goods and services account for an increasing share in Latvian exports but research capabilities remain low

The share of ICT services in total business services exports increased significantly between 2010 and 2015, rising from 3.6% to 6%. While ICT services export intensity was higher in neighbouring Estonia (8.3%), Latvia overtook both Denmark (5.3%) and Norway (5.7%) (Figure 6.23). Between 2010 and 2015, Latvia also further developed an RCA in value-added exports of IT and other information services (Figure 6.14). However, research and development expenditures as a share of total value added (0.5% in 2015) remained significantly below the OECD average (4.8%) for ICT services.

Figure 6.23. ICT services[1] exports from Latvia and selected OECD countries, 2010-15

As a percentage of all business sector[2] exports



1. ICT services relate to D62-D63 (ISIC, Rev.4), IT and other information services.

2. Business sector services (D45-D82) exclude real estate.

Source: OECD (2020f), "STAN Industry ISIC Rev. 4", *https://dx.doi.org/10.1787/data-00649-en* (accessed on 24 February 2020).

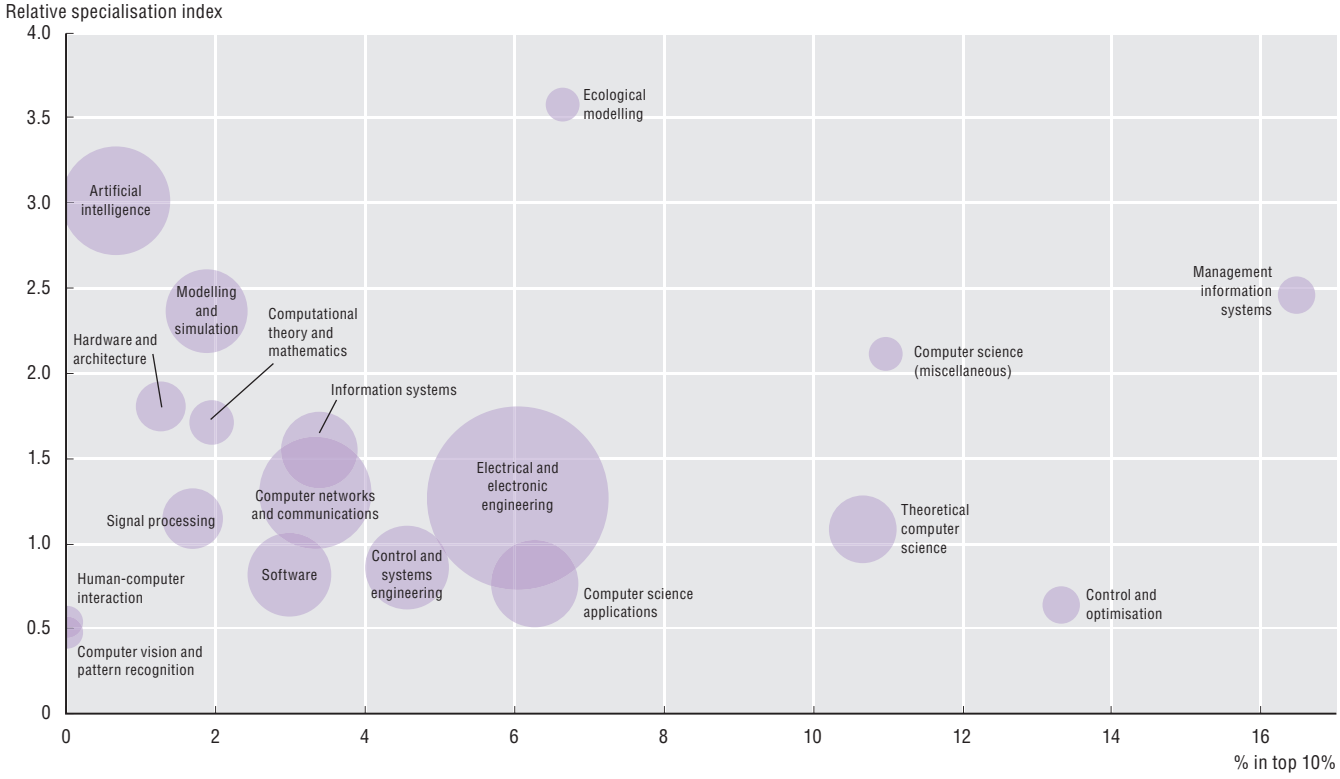
The ICT and electronic goods sector has also grown rapidly over recent years. Between 2010 and 2017, the share of Computer, electronic and optical products in total manufacturing value added more than doubled, from 2.2% to 4.9% (Figure 6.12). A similar increase can be observed for manufacturing exports, where the share of the sector aggregate grew from 3% to 6.3% between 2010 and 2018 (Figure 6.17).

Large increases in exports were observed for product categories such as transmission apparatus (radio, telephone or TV), monitors and projectors, microphones and printed circuits. Jointly, these products accounted for over three-quarters of total ICT goods exports in 2018.[10] However, despite progress since 2010, Latvia had not attained an RCA for the sector aggregate in 2015 (Figure 6.13). Additionally, research and development expenditures for computer, electronic and optical products as a share of value added (2.5%) also remained significantly below the OECD average (23.7%) (Figure 6.15).

Patent applications nevertheless suggest increasing research activity in areas related to audio-visual technologies and computer technology. Together, these patent classes accounted for 8.9% of all applications in 2012-16, up from 1.9% in 2007-11. Applications in related areas (e.g. telecommunications, basic communication processes, semi-conductors or digital communication) declined (from 5.4% to 2.4%).[11]

Figure 6.24. Latvia's publications in the top 10% most cited documents on computer science, electronic engineering and related fields

Average, 2014-18



Note: Excludes fields with less than five publications between 2014 and 2018. Number (fractional) of publications ranges from 8.8 (Human-computer interaction) to 281 (Electrical and electronic engineering). See Figure 6.18 for more details.

Source: OECD calculations based on Elsevier, Scopus Custom Data, Version 5.2019.

The share of top-cited scientific publications in most fields of computational science and electronic engineering remained below 10%, the global average across countries (Figure 6.24). The exception consisted of a small number of highly cited publications in theoretical computer science (e.g. quantum computing or management information systems). Specialisation is strong in the field of artificial intelligence, with around 100 publications in 2014-18. However, only 0.7% were among the top 10% in terms of citations. As mentioned above, a large number of publications were published in the field of electronic engineering, but only 6% were among the 10% most cited documents, below the global average (10% by definition).

These findings suggest room to further strengthen research capacity and specialisation, both in general fields, such as artificial intelligence, and fields with clear applications in other Smart Specialisation areas, such as health informatics or ecological modelling.

Government support lacks a focus on Smart Specialisation areas

The ICT Smart Specialisation area accounted for about 17.4% of funding from instruments available under the Smart Specialisation Strategy (Table 6.2). As the area is considered to have a substantial cross-sectoral impact – like Smart Energy, which received 27.5% of the total funding – the low share of resources allocated is surprising. Programmes fostering research commercialisation and the competence centres for ICTs accounted for a relatively larger share of the available funds for the area, whereas funding for fundamental and applied research, post-doctoral research or practical research was relatively low. Thus, while ICT research in the early stages (TRL 1-3) received only EUR 12.5 million in 2014-18, funding reached EUR 29.1 million for Smart Materials and 33.4 million for Biomedicine (Table 6.2).

Funding has also been scattered across many fields. Around 32% of the total ICT funds available were distributed among ICT goods, including smart sensors and the Internet of Things (11.1%), robotics and computer vision (4.6%), and a wide array of electronics (16.3%) ranging from smart screens, semi-conductors and microchips, to smart cars, 3D printers, audio devices and precision instruments (Table 6.4). More targeted funds went to computational linguistics and machine translation (14.5%). The remainder was distributed among a diverse set of research areas, including education technologies, quantum research, space technologies, business process management, big data and cyber security. As a result, specific fields of high relevance to Smart Specialisation value chains received rather limited funding. For example, medical informatics and bioinformatics were considered jointly with other big data applications, which taken together received only 8.6% of the available funds.

Table 6.4. Support for ICTs does not align with needs of other Smart Specialisation areas

Funds for Smart Specialisation in the area of ICT, 2014-18

Research areas	Funding instruments of the Ministry of Education and Science			EU Innovation and research programme	Funding instruments of the Ministry of Economics	
	National/ government funding	EU funds (e.g. ESIF, ERDF)	EU funds (e.g. ESIF, ERDF)	Horizon 2020	EU funds (e.g. ESIF, ERDF)	EU funds (e.g. ESIF, ERDF)
	Fundamental and applied research programme	Post-doctoral research (1.1.1.2.)	Practical research (1.1.1.1.)	Horizon 2020	Research results commercialisation (1.2.1.2.)	Competence Centres (1.2.1.1.)
	TRL 1-2	TRL 1-2	TRL 2-3	TRL 4-8	TRL 3-5	TRL 4-6
Computational linguistics	495 446	133 806	1 338 661	1 375 750	x	1 419 752
Algorithms	698 910	802 836	921 276	x	23 572	1 134 227
Machine learning	699 874	267 612	x	17 339	x	830 155
Education technologies and digitalisation	200 000	401 418	1 837 020	x	x	x
Business process management systems	x	x	x	533 663	x	1 647 396
Electronics	x	x	517 036	1 064 329	x	3 778 490
Smart sensors and Internet of Things	300 000	1 070 448	x	1 553 216	730 743	x
Robotics	300 000	267 612	x	550 560	332 936	62 500
Big data	x	401 418	x	1 669 115	681 584	x
Data storage, transmission and systems	x	401 418	x	246 561	x	1 835 455
Space technologies and remote sensing	799 973	66 903	624 449	100 000	326 850	x
Public and cyber security	x	x	x	401 085	x	72 946
Total	**3 494 203**	**3 813 470**	**5 238 442**	**7 511 618**	**2 095 685**	**10 780 921**

Notes: x = not applicable. Computational linguistics includes research in the area of machine translation. Algorithms includes quantum research. Robotics includes computer vision research. Big data includes medical informatics/bioinformatics research. Electronics includes research in several fields, including smart screens, semi-conductors, microchips, smart cars, 3D printers, and audio or precision devices.

Source: OECD, based on data from the MoES.

The current funding structure, therefore, does not sufficiently support the role of applied ICT research as a fundamental enabler for other specialisation areas. In particular, more targeted funding could help support emerging ecosystems in other Smart Specialisation areas, including specialised research on Integrated Computational Materials Engineering (ICME), environmental modelling, bioinformatics

or health informatics. Fostering modular programmes (see Chapter 4) and more strongly involving engineers and ICT specialists in the research projects of applied institutes, such as the Laboratory for Genomics and Bioinformatics at LU or the Faculty of Materials Science and Applied Chemistry at RTU, could assist in this regard. Additionally, newly installed infrastructure, such as the Microsoft Innovation Centre (LUMIC), should be leveraged to foster emerging Smart Specialisation ecosystems. Bringing international researchers to Latvia, including through conferences such as the 15th International Conference on Agricultural Informatics and Communication (2021 in Riga), would also support this approach.

The IT sector requires broad-based policy support

Particular clusters of excellence in the Latvian ICT sector have attracted significant Horizon 2020 funding. Currently, 36 signed grants benefit from H2020 funding of almost EUR 7.9 million. After Food and Energy, ICT projects were the third most important area of H2020 funding for Latvia. Several projects have arisen in the area of computational linguistics and machine translation. These include SUMMA (Scalable Understanding of Multilingual Media), which received contributions of EUR 1.2 million, making it the largest H2020 project with a focus on ICTs. The project ran from 2016 to 2019 and involved the Latvian Information Agency (LETA) along with research institutions in four other European countries.

Together with 12 other firms and research institutions, LETA was also one of the founders of the first IT Competence Centre (IT CC) programme in 2010, one of the main focuses of which was language technology. Tilde SIA, another co-founder of IT CC, was also involved in several H2020 projects focused on machine translation. The two most recent projects, co-ordinated in France and Germany, respectively, received funding of EUR 935 000 up to 2021. Tilde's machine translation technology, which specialises in Baltic languages, has outperformed solutions from key players such as Google and Microsoft in the translation of Lithuanian, Estonian and Latvian (LSM, 2019). The technology is freely available for the three Baltic languages as well as Arabic, English, Finnish, Polish and Russian.

Other successful deep-tech firms have also benefited from the Competence Centre programme. For example, as part of the IT CC, the company Squalio developed a deep-tech solution for vehicle licence plate recognition and applied it to speed cameras in a pilot with the Latvian Traffic Safety Directorate (CSDD). According to the CSDD, the solution has already reduced the number of car accidents and is a good example of how smart procurement can be used to foster technological innovation. In another example, Tilde was awarded a tender in 2017 by a Directorate (G3) of the European Commission for the provision of tools and resources for automated translation and language processing services.

Latvian deep tech is likely to evolve further in the future, with firms like Tilde or Squalio generating awareness of particular technological niches. In addition, the Latvian IT Cluster has recently attracted additional H2020 funds for a programme to help deep-tech start-ups improve products and sell more effectively (STARTUP3). However, while H2020 or competence centres can help develop particular technological niches, they need to be complemented by more comprehensive policy measures to support innovation.

Countries have introduced several measures to support the growth of ICT sectors, including loans, export or innovation subsidies, training, and ICT specific incubators and accelerators (OECD, 2019o). Measures to foster the adoption of digital technologies (see Chapter 4) also play an important role in creating demand for domestic solutions. Latvia should consider strategies to ease the demand for skills and enhance productivity in the sector. In addition to making adjustments to the education system, such strategies could involve measures to attract ICT specialists from abroad. In Belgium, a special tax regime for foreign executives and specialists has provided benefits to foreigners with particular skills on a temporary basis since 1983. In Germany, the government has recently agreed a plan with business leaders to ease entry into the country for foreign workers. The resulting Memorandum of Understanding foresees support from the German bureaucracy, assistance with the search for housing and faster visa processes.

The design and implementation of regulatory adjustments will be crucial in particular sectors. For example, ICT firms developing Fintech solutions are likely to benefit significantly from the creation of regulatory sandbox environments or the swift and coherent implementation of emerging regulation. For example, the Alternative Financial Services Association of Latvia, which represents several Latvian

Fintech firms, has joined forces with associations in Denmark, Poland and Spain to voice concerns over the increasing difficulties associated with small sum, cross-border lending. The coalition, which represents over 100 digital lenders, argues that the implementation of existing EU rules, such as the Consumer Credit Directive, varies widely across different member states and is stifling market entry by foreign competitors. In response, the European Commission is currently evaluating the need to revise the Consumer Credit Directive. In this and other similar cases, the Latvian government should foster ongoing dialogue with sector representatives and – in the case of EU regulation – with other countries, to determine how regulation can be implemented without creating unnecessary friction.

Box 6.14. Policy Recommendations: ICT

- Re-allocate Smart Specialisation funding towards the ICT specialisation area to better account for the positive spill-over effects ICTs generate across the economy, including in other Smart Specialisation areas.
- Concentrate funding in selected niches of excellence (e.g. machine translation, audio technology), as well as research fields complementary to other Smart Specialisation areas (e.g. health informatics).
- Complement targeted instruments with broader support for ICT innovation and adoption, and consider the introduction of special tax regimes or relocation support to attract foreign ICT specialists.
- Foster dialogue with sector representatives to ensure that emerging regulation is implemented without creating unnecessary friction.

References

ALTUM (2019), "The first 18 startups financed by the ALTUM accelerator programs graduate most promising teams will qualify for 250 thousand euro investment", *www.altum.lv/en/news/veiksmigi-nosledzies-pirmais-posms-altum-akceleratoru-programma-daudzsolosakie-jaunuznemumi-pretende-uz-250-tukstosu-eiro-ieguldijumu* (accessed in March 2020).

Appelt, S. et al. (2016), "R&D tax incentives: Evidence on design, incidence and impacts", *OECD Science, Technology and Industry Policy Papers*, No. 32, OECD Publishing, Paris, *https://dx.doi.org/10.1787/5jlr8fldqk7j-en*.

Beckerman-Rodau, A. (2011), "The problem with intellectual property rights: Subject matter expansion", *Yale Journal of Law and Technology*, Vol. 13/1, pp. 36-89.

Cross-Sectoral Coordination Centre (2019), *National Development Plan of Latvia for 2021-2027*, first version summary, Riga.

Cross-Sectoral Coordination Centre (2017), *National Development Plan 2014-2020 Annual And Sustainable Development Strategies For Latvia Up To 2030. Annual Implementation Monitoring Report*, Riga.

CSBL (2020a), *IKG10_060 Total Gross Value Added by Kind of Activity (NACE Rev. 2)* (database), Central Statistical Bureau of Latvia, Riga, *https://data1.csb.gov.lv/pxweb/en/ekfin/ekfin__ikp__IKP__ikgad*.

CSBL (2020b), *Exports and Imports by Commodity Section and by Economic Activity (NACE Rev.2) of the Importer (thsd euro) – ATG015* (database), Central Statistical Bureau of Latvia, Riga, *www.csb.gov.lv/en/statistics/statistics-by-theme/foreign-trade/ft-nace-bec/tables/atg015/exports-and-imports-commodity-section-and*.

CFCA (2020), "History", Central Finance and Contracting Agency, Riga, *www.cfla.gov.lv/en/about-us/history* (accessed on 20 May 2020).

CFCA (2019), "General information," Central Finance and Contracting Agency, Riga, *www.cfla.gov.lv/en/eu-funds-2014-2020/general-information* (accessed on 20 May 2020).

Deloitte (2018), *Using Public-Private Partnerships to Advance Smart Cities. Part 2: Funding and Financing Smart Cities Series*, Deloitte Center for Government Insights, New York, NY, *www2.deloitte.com/content/dam/Deloitte/global/Documents/Public-Sector/gx-ps-public-private-partnerships-smart-cities-funding-finance.pdf*.

Eichler, H-G. et al. (2019), "Data rich, information poor: Can we use electronic health records to create a learning healthcare system for pharmaceuticals?" *Clinical Pharmacology and Therapeutics*, Vol. 105/4, pp. 912-922, *doi:10.1002/cpt.1226*.

EsFondi.lv (2020a), "Informācijas sistēmu modelēšanas principu piemērošana strukturētai un mērķtiecīgai kompetenču pārvaldībai" [Application of information systems modeling principles to structured and purposeful competence management], *www.esfondi.lv/es-fondu-projektu-mekletajs/project?number=1.1.1.1%2F16%2FA%2F252* (accessed in March 2020).

EsFondi.lv (2020b), "Neironu tīkli fleksīvo dabisko valodu apstrādei" [Neural networks for processing flexible natural languages], *www.esfondi.lv/es-fondu-projektu-mekletajs/project?number=1.1.1.1%2F16%2FA%2F215* (accessed in March 2020).

EsFondi.lv (2020c), "Informācijas un komunikācijas tehnoloģiju kompetences centrs" [Information and Communication Technology Competence Centre], *www.esfondi.lv/es-fondu-projektu-mekletajs/project?number=1.2.1.1/18/A/003* (accessed in May 2020).

EsFondi.lv (2020d), "Tehnoloģiju pārneses programma" [Technology transfer programme], *www.esfondi.lv/es-fondu-projektu-mekletajs/project?number=1.2.1.2%2F16%2FI%2F001* (accessed in May 2020).

EsFondi.lv (2020e), "RTU inovāciju granti studentiem" [RTU innovation grants for students], *www.esfondi.lv/es-fondu-projektu-mekletajs/project?number=1.1.1.3/18/A/001* (accessed in May 2020).

European Commission (2020), *Country Report Latvia 2020*, Commission Staff Working Document, Brussels, *https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1584543810241&uri=CELEX%3A52020SC0513*.

European Commission (2018a), *The Latvian Research Funding System*, Brussels, *https://op.europa.eu/en/publication-detail/-/publication/f631a55b-bbba-11e8-99ee-01aa75ed71a1*.

European Commission (2018b), *Digital Innovation Hubs – Smart Specialisation Platforms, Brussels*, *https://s3platform.jrc.ec.europa.eu/digital-innovation-hubs-tool/-/dih/13295/view* (accessed in February 2020).

European Commission (2018c), "Latvia – S3 priorities as encoded in the 'Eye@RIS3' Tool", Smart Specialisation Platform, Version: 1.0.47, Brussels, *https://s3platform.jrc.ec.europa.eu/regions/LV/tags/LV* (accessed on 30 September 2019).

European Commission (2017), *Latvian Research Funding System Background Report: Horizon 2020 Policy Support Facility*, European Commission, Brussels, *http://dx.doi.org/10.2777/4162*.

European Commission (2013), *The Role of Clusters in Smart Specialisation Strategies*, European Commission, Directorate-General for Research and Innovation, Brussels, *https://ec.europa.eu/research/evaluations/pdf/archive/other_reports_studies_and_documents/clusters_smart_spec2013.pdf*.

European Commission (2012a), *Latvia: National Industrial Policy Guidelines for 2014-2020*. Digital Transformation Monitor, European Commission, Brussels, *https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Latvia_vf.pdf*.

European Commission (2012b), *Guide to Research and Innovation Strategies for Smart Specialisation (RIS 3)*, Regional Policy, European Commission, Brussels, *http://s3platform.jrc.ec.europa.eu/documents/20182/84453/RIS3+Guide.pdf/fceb8c58-73a9-4863-8107-752aef77e7b4*.

European Commission/OECD (2020), *STIP Compass: International Database on Science, Technology and Innovation Policy (STIP)*, European Commission, Brussels, OECD, Paris, *https://stip.oecd.org*.

Eurostat (2020a), *ICT Usage in Enterprises – E-business (isoc_eb)* (database), *https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/database*.

Eurostat (2020b), "Renewable Energy Statistics", Eurostat Statistics Explained, *https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Renewable_energy_statistics#Share_of_renewable_energy_almost_doubled_between_2004_and_2018* (accessed on 10 June 2020).

Eurostat (2020c), *Patent Applications to the EPO by Priority Year* (database), *https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=pat_ep_ntot&lang=en* (accessed on 6 May 2020).

Eurostat (2019), *Education Administrative Data from 2013 Onwards* (database), *https://ec.europa.eu/eurostat/cache/metadata/en/educ_uoe_enr_esms.htm*.

Eurostat (2016), *Community Innovation Survey (CIS-2016)* (database), *https://ec.europa.eu/eurostat/web/microdata/community-innovation-survey*.

FAO (2020), *Forestry Production and Trade* (database), *www.fao.org/faostat/en/#data/FO/visualize* (accessed on 20 May 2020).

FFG (2015), *Service Innovations – Funding Guidelines*, Austrian Research Promotion Agency, Vienna, *www.ffg.at/en/programme/service-innovations* (accessed in March 2020).

Galindo-Rueda, F. and F. Verger (2016), "OECD taxonomy of economic activities based on R&D intensity", *OECD Science, Technology and Industry Working Papers*, No. 2016/4, OECD Publishing, Paris, *https://dx.doi.org/10.1787/5jlv73sqqp8r-en*.

Government of Latvia (2013), *Guidelines for Science, Technology Development, and Innovation 2014-2020*, Riga, *https://s3platform.jrc.ec.europa.eu/documents/20182/227021/Guidelines+for+Science+Technology+and+Innovation+2014-2020.pdf/d96566cd-e61b-471b-9f80-4d06236037b4*.

Grinfelds, T. (2018), "Industry trends and challenges in Latvia", presentation for Digital Transformation of the Engineering Industries in the Baltic Sea region – Conference in the framework of "Tech Industry 2018", *https://veca.likta.lv/EN/Documents/TomsGrinfelds-MASOC.pdf* (accessed on 3 October 2019).

IEA (2019a), *World Energy Balances* (database), International Energy Agency, Paris, *www.iea.org/statistics/?country=LVA&isISO=true*.

IEA (2019b), *World Energy Prices*, International Energy Agency, Paris, *http://data.iea.org/payment/products/121-world-energy-prices-2019-edition.aspx*.

IEA (2017), *Digitalisation and Energy*, International Energy Agency, Paris, *www.iea.org/reports/digitalisation-and-energy*.

Lauma Muizniece, A. (2017), "Supporting university technology transfer-struggles and barriers in Latvia", *Ekonomska misao i praksa*, Vol. 26/1, pp. 321-342.

LIDA (2019a), "Inovāciju motivācijas programma" [Innovation motivation programme], Investment and Development Agency of Latvia, Riga, *www.liaa.gov.lv/lv/fondi/2014-2020/inovaciju-motivacijas-programma*.

LIDA (2019b), "Innovation Voucher Program: Financial boost for empowering innovation", Investment and Development Agency of Latvia, Riga, *https://startuplatvia.eu/innovation-voucher*

LIDA (2019c), "Inovāciju vaučeru atbalsta pakalpojumi" [Innovation voucher support services], Investment and Development Agency of Latvia, Riga, *www.liaa.gov.lv/lv/fondi/2014-2020/inovaciju-vauceru-atbalsta-pakalpojumi*.

LIDA (2019d), "Start-up ecosystem", Investment and Development Agency of Latvia, Riga, *www.liaa.gov.lv/en/invest-latvia/start-up-ecosystem* (accessed in October 2019).

LIDA (2019e), "Incentives for R&D", Investment and Development Agency of Latvia, Riga, *www.liaa.gov.lv/en/invest-latvia/investor-business-guide/incentives-investors/incentives-rd* (accessed in October 2019).

LIDA (2019f), "Magnetic Latvia business incubators", Investment and Development Agency of Latvia, Riga, *https://startuplatvia.eu/magnetic-latvia-business-incubators* (accessed in October 2019).

LIDA (2019g), "Startup visa application process", Investment and Development Agency of Latvia, Riga, *https://startuplatvia.eu/files/resources/editor/LV%20Startup%20Visa%20Application%20Process%202019.10.09.pdf*.

LIDA (2019h), "Life sciences", Investment and Development Agency of Latvia, Riga, *www.liaa.gov.lv/en/invest-latvia/sectors-and-industries/life-sciences* (accessed on 5 December 2019).

LSM (2019), "Latvia's Tilde beats Internet giants in machine translation battle", *LSM.lv*, *https://eng.lsm.lv/article/society/education/latvias-tilde-beats-internet-giants-in-machine-translation-battle.a327904* (accessed on 18 October 2019).

Magnetic Latvia (2019), "Startup law benefits", *https://startuplatvia.eu/startup-law-benefits*.

MGI (2019), "BGI Group and European Partners launch project to sequence and analyze 10 million cells", *MGI News Center*, *https://en.mgitech.cn/news/108* (accessed on 17 February 2020).

MoA (2018), *Latvian Bioeconomy Strategy 2030 – Informative Report*, Ministry of Agriculture, Riga, *www.zm.gov.lv/public/files/CMS_Static_Page_Doc/00/00/01/46/58/E2758-LatvianBioeconomyStrategy2030.pdf*.

MoE (2018a), "Clusters", Ministry of Economics, Riga, *www.em.gov.lv/en/sectoral_policy/industrial_policy/clusters*.

MoE (2018b), *Economic Development of Latvia*, Ministry of Economics, Riga, *www.em.gov.lv/files/tautsaimniecibas_attistiba/leap/leap_2018-en.pdf*.

MoE (2018c), "Assessment of Latvian start-up ecosystem, description of the current situation and recommendations for further improvements", Ministry of Economics, Riga.

MoES (2020a), "Latvijā tiek veidota vienota un spēcīga zinātnes politikas ieviešanas iestāde" [A unified and strong science policy implementation institution is being established in Latvia]", Ministry of Education and Science, Riga, *www.izm.gov.lv/lv/aktualitates/4002-latvija-tiek-veidota-vienota-un-speciga-zinatnes-politikas-ieviesanas-iestade* (accessed on 14 May 2020).

MoES (2020b), *RIS3 Info on Investments in RIS3 by Instrument (2014-2018)*, Ministry of Education and Science, Riga.

MoES (2018), *Informative Report: Monitoring of Smart Specialization Strategy*, Ministry of Education and Science, Riga, *https://s3platform.jrc.ec.europa.eu/documents/20182/0/RIS3_progress+report_LV_2018.pdf/940176c6-b886-4213-9f18-75c20251bfb9*.

MoES (2015), *Analytical Description of the Ecosystem of Smart Specialization Area "Smart Energetics"*, Ministry of Education and Science, Riga, *https://cfla.gov.lv/userfiles/files/1111_Ecosystem%20-%20Smart%20energetics.docx*.

MoES (2013a), *About the development of Smart Specialisation Strategy*, Ministry of Education and Science, Riga, *www.izm.gov.lv/images/zinatne/RIS3_ENG/The_Informative_Report_Development_of_RIS3.pdf*.

MoES (2013b), *Assessment of Export Potential of Economic Sectors*, Appendix 2 to the informative report "On the Development of Smart Growth Strategy and Determination of Specialisation", Ministry of Education and Science, Riga, *www.riseba.lv/sites/default/files/inline-files/Appendix_2_Assessment_of_Export_Potential_of_Economic_Sectors.pdf*.

MoF (2020), *Vadlīnijas par finanšu korekciju piemērošanu, ziņošanu par Eiropas Savienības fondu ieviešanā konstatētajām neatbilstībām, neatbilstoši veikto izdevumu atgūšanu 2014.-2020.gada plānošanas period* [Guidelines on the application of financial corrections, reporting on discrepancies identified in the implementation of European Union funds, recovery of irregularly incurred expenditure in the 2014-2020 programming period], Ministry of Finance, Riga, *www.esfondi.lv/upload/Vadlinijas/vadlinijas_10022020.zip*.

MoH (2019), "Veselības ministre uz laiku apturējusi e-veselības trešās kārtas uzsākšanu", [Minister of Health Temporarily Suspended the Launch of the Third Round of e-Health], Ministry of Health, Riga, *www.vm.gov.lv/lv/aktualitates/preses_relizes/5946_veselibas_ministre_uz_laiku_apturejusi_eveselibas_tresas_kar* (accessed on 14 October 2019).

Miroudot, S. and C. Cadestin (2017), "Services in global value chains: Trade patterns and gains from specialisation", *OECD Trade Policy Papers*, No. 208, OECD Publishing, Paris, *https://dx.doi.org/10.1787/06420077-en*.

Nye Forretningsmodeller (2019), "One Stop Shop for new business models", Copenhagen, *https://nyeforretningsmodeller.dk/english* (accessed in February 2020).

Oderkirk, J. (2017), "Readiness of electronic health record systems to contribute to national health information and research", *OECD Health Working Papers*, No. 99, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9e296bf3-en*.

OECD (forthcoming), *Regulatory Aspects of Data Governance for the Digital Transformation of Agriculture*, OECD Publishing, Paris.

OECD (2020a), *FDI Stocks* (indicator), OECD Publishing, Paris, *https://dx.doi.org/10.1787/80eca1f9-en* (accessed on 28 February 2020).

OECD (2020b), *Main Science and Technology Indicators* (database), OECD, Paris, *www.oecd.org/sti/msti.htm* (accessed on 28 February 2020).

OECD (2020c), *The Digitalisation of Science, Technology and Innovation: Key Developments and Policies*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/b9e4a2c0-en*.

OECD (2020d), "Trade in value added", *OECD Statistics on Trade in Value Added* (database), OECD, Paris, *https://dx.doi.org/10.1787/data-00648-en* (accessed on 27 February 2020).

OECD (2020e), "Research and development statistics: Business enterprise R-D expenditure by industry – ISIC Rev. 4", *OECD Science, Technology and R&D Statistics* (database), OECD, Paris, *https://dx.doi.org/10.1787/data-00668-en* (accessed on 13 March 2020).

OECD (2020f), "STAN Industry ISIC Rev. 4", *STAN: OECD Structural Analysis Statistics* (database), OECD, Paris, *https://dx.doi.org/10.1787/data-00649-en* (accessed on 24 February 2020).

OECD (2020g), "Research and development statistics: Gross domestic expenditure on R-D by sector of performance and source of funds", *OECD Science, Technology and R&D Statistics* (database), OECD, Paris, *https://dx.doi.org/10.1787/data-00189-en* (accessed on 26 February 2020).

OECD (2020h), "Patents by main technology and by International Patent Classification (IPC)", *OECD Patent Statistics* (database), OECD, Paris, *https://dx.doi.org/10.1787/data-00508-en* (accessed on 17 March 2020).

OECD (2020i), *Smart Cities and Inclusive Growth*, OECD, Paris, *www.oecd.org/cfe/cities/OECD_Policy_Paper_Smart_Cities_and_Inclusive_Growth.pdf*.

OECD (2019a), *OECD Economic Surveys: Latvia 2019*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/f8c2f493-en*.

OECD (2019b), *Business Innovation Statistics and Indicators* (database), OECD, Paris, *http://oe.cd/inno-stats*.

OECD (2019c), *Education at a Glance 2019: OECD Indicators*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/f8d7880d-en*.

OECD (2019d), *Digital Innovation: Seizing Policy Opportunities*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/a298dc87-en*.

OECD (2019e), *OECD Reviews of Digital Transformation: Going Digital in Colombia*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/781185b1-en*.

OECD (2019f), *R&D Tax Incentives* (database), OECD, Paris, *www.oecd.org/sti/rd-tax-stats.htm*.

OECD (2019g), *Innovation, Agricultural Productivity and Sustainability in Latvia*, OECD Food and Agricultural Reviews, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264312524-en*.

OECD (2019h), *OECD SME and Entrepreneurship Outlook 2019*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/34907e9c-en*.

OECD (2019i), "Country Snapshots: Latvia", in *Financing SMEs and Entrepreneurs 2019: An OECD Scoreboard*, OECD Publishing, Riga, *https://doi.org/10.1787/fin_sme_ent-2019-en*.

OECD (2019j), *Regions in Industrial Transition: Policies for People and Places*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/c76ec2a1-en*.

OECD (2019k), *Benchmarking Higher Education System Performance, Higher Education*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/be5514d7-en*.

OECD (2019l), *Latvia: Country Health Profile 2019, State of Health in the EU,* OECD Publishing, Paris/European Observatory on Health Systems and Policies, Brussels, *https://dx.doi.org/10.1787/b9e65517-en*.

OECD (2019m), *OECD Environmental Performance Reviews: Latvia 2019*, OECD Environmental Performance Reviews, OECD Publishing, Paris, *https://dx.doi.org/10.1787/2cb03cdd-en*.

OECD (2019n), *Enhancing the Contribution of Digitalisation to the Smart Cities of the Future*, OECD Publishing, Paris, *www.oecd.org/cfe/regional-policy/Smart-Cities-FINAL.pdf*.

OECD (2019o), "ICT investments in OECD countries and partner economies: Trends, policies and evaluation", *OECD Digital Economy Papers*, No. 280, OECD Publishing, Paris, *https://doi.org/10.1787/bcb82cff-en*.

OECD (2019p), "Harnessing data to manage biomedical technologies", in *Health in the 21st Century: Putting Data to Work for Stronger Health Systems*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/1df03c3b-en*.

OECD (2019q), "Innovation support in the enterprise sector", *OECD Science, Technology and Industry Policy Papers*, OECD Publishing, Paris, *https://doi.org/10.1787/4ffb2cbc-en*.

OECD (2019r), *Digital Opportunities for Better Agricultural Policies*, OECD Publishing, Paris, *https://doi.org/10.1787/571a0812-en*.

OECD (2018a), "R&D tax incentives: Latvia, 2017", OECD, Paris, *www.oecd.org/sti/rd-tax-stats-latvia.pdf*.

OECD (2018b), "Effective operation of competitive research funding systems", *OECD Science, Technology and Industry Policy Papers*, No. 57, OECD Publishing, Paris, *https://dx.doi.org/10.1787/2ae8c0dc-en*.

OECD (2018c), *OECD Reviews of Digital Transformation: Going Digital in Sweden*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264302259-en*.

OECD (2017a), *OECD Economic Surveys: Latvia 2017*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/eco_surveys-lva-2017-en*.

OECD (2017b), *OECD Territorial Reviews: Northern Sparsely Populated Areas*, OECD Territorial Reviews, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264268234-en*.

OECD (2017c), *The Next Production Revolution: Implications for Governments and Business*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264271036-en*.

OECD (2017d), *Public Procurement for Innovation: Good Practices and Strategies*, OECD Public Governance Reviews, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264265820-en*.

OECD (2016), *Education in Latvia, Reviews of National Policies for Education*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264250628-en*.

OECD (2011), "Nordic countries: Matching exceptional design and creativity with progressive policy", in *Intellectual Assets and Innovation: The SME Dimension,* OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264118263-6-en*.

Ozols, G. (2018), "Cooperation on data driven nation development in Latvia", *Joinup*, Brussels, *https://joinup.ec.europa.eu/collection/egovernment/document/cooperation-data-driven-nation-development-latvia* (accessed on 22 August 2019).

Patent Office of the Republic of Latvia (2019), "Intellectual Property Information Centre", Riga, *www.lrpv.gov.lv/en/patent-and-technology-library/patent-and-technology-library* (accessed on October 2019).

Paunov, C. and S. Planes-Satorra (2019), "How are digital technologies changing innovation?: Evidence from agriculture, the automotive industry and retail", *OECD Science, Technology and Industry Policy Papers*, No. 74, OECD Publishing, Paris, *https://dx.doi.org/10.1787/67bbcafe-en*.

PPKK (2019), "Digitalisation is at the base of growth – new digitalisation workshops are launched, specifically designed for the food industry", PPKK.lv, *www.ppkk.lv/en/international-activities* (accessed on 2 October 2019).

Productivity Commission (2017), *Data Availability and Use*, Productivity Commission Inquiry Report, No. 82, Australian Government, Canberra, *www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf*.

Rovite, V. et al. (2018), "Genome Database of the Latvian Population (LGDB): Design, goals, and primary results", *Journal of Epidemiology*, Vol. 28/8, pp. 353-360, *http://dx.doi.org/10.2188/jea.je20170079*.

RTU (2019), "RTU Innovation Grants for Students", rtu.lv, *www.rtu.lv/en/university/rtu-projects/open?project_number=3912* (accessed on 13 May 2020).

RVO (2018), Service Design Vouchers, Agency, N. (ed.), *www.rvo.nl/subsidies-regelingen/service-design-vouchers* (accessed in March 2020).

SENAR (2016), "SENAR-MT Lança Treinamento Sobre Operação de Drones na Agropecuária" [SENAR-MT Launches Training on Drone Operation at Agropecuári], Agro de Precisão.

Strods, J. (2017), "Smart city solutions for small city", Jelgava City Council presentation, *www.norden.lv/Uploads/2017/09/11/1505122734_.pdf* (accessed on 23 February 2020).

Swedish Ministry of Education and Research (2019), *Swedish National Roadmap for the European Research Area 2019–2020*, Stockholm, *www.government.se/4adab0/contentassets/514bde7beb4d423ea7b7b1f2c50f470f/swedish-national-roadmap-for-era-2019-2020.pdf*.

Takalo, T. (2013), "Rationales and instruments for public innovation policies", *Bank of Finland Research Discussion Papers*, Vol. 1/2013, *http://dx.doi.org/10.2139/ssrn.2217502*.

Vaivare, L (2018a), "Miracle tree", *Innovation*, Vol. 3/Summer, Magnetic Latvia, *https://startuplatvia.eu/sites/default/files/resurs_file/InnovationMag3_2018_0.pdf* (accessed on 10 October 2019).

Vaivare, L. (2018b), "Life with a plastic bag on your head", *Innovation*, Vol. 5/Autumn/Winter, Magnetic Latvia, *https://startuplatvia.eu/files/resources/resource_file/innovation_journal.pdf* (accessed on 15 October 2019).

WITS/UN Comtrade (2020), *UNSD Commodity Trade* (database), *http://wits.worldbank.org* (accessed on 4 February 2020)

The World Bank (2018a), *Focus on Performance – World Bank Support to Higher Education in Latvia, Volume 2: Internal Funding and Governance*, The World Bank, Washington, DC.

The World Bank (2018b), *Focus on Performance –World Bank Support to Higher Education in Latvia, Volume 3: Academic Careers*, The World Bank, Washington, DC.

Notes

Israel

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

1. The ERDF is one of five European Structural and Investment Funds (ESIF). The other funds are: the European Social Fund (ESF), the Cohesion Fund (CF), the European Agricultural Fund for Rural Development (EAFRD) and the European Maritime and Fisheries Fund (EMFF).
2. The OECD defines smart cities as "initiatives or approaches that effectively leverage digitalisation to boost citizen well-being and deliver more efficient, sustainable and inclusive urban services and environments as part of a collaborative, multi-stakeholder process" (OECD, 2020i). The smart city definition of the Latvian Ministry of Environmental Protection and Regional Development can be found in the same document.

3. The (value-added) RCA is defined as the share of value-added originating from a given sector in a country's exports divided by the share of value-added originating from this sector in world exports. In a world without any trade distortion, the RCA would be a good proxy for what economists define as comparative advantage. A country has a comparative advantage in a sector when this share is above 1 (i.e. when the value-added coming from this sector represents a higher share for this country as compared to the world average) (see Miroudot and Cadestin, 2017).
4. Changes in the export value over time do not fully account for specific price changes of products within the export basket. Possible developments in wood chemistry and new biomaterials (see below) are not captured in these figures.
5. R&D expenditure directed towards the bioeconomy also arises in fields such as engineering and technology, for example in relation to process innovations or new machinery.
6. Calculations are based on OECD (2020h) and consider patent applications filed under the Patent Cooperation Treaty (PCT), using the priority data and the inventor's country of residence as defining characteristics. Counts are based on the list of IPC codes given in each patent document, and use fractional counts.
7. Precise data for the government sector are not available for 2016 due to confidentiality reasons.
8. OECD calculations based on OECD (2020h).
9. The strategic use of public procurement for innovation is defined as any kind of public procurement practice (pre-commercial or commercial) that is intended to stimulate innovation through research and development and the market uptake of innovative products and services (OECD, 2017d).
10. OECD calculations based on WITS/UN Comtrade (2020).
11. OECD calculations based on OECD (2020h).

Chapter 7

POLICIES FOR DIGITAL TRANSFORMATION: RECOMMENDATIONS FOR A WHOLE-OF-GOVERNMENT APPROACH

Going Digital in Latvia: An Integrated Policy Framework

The previous chapters of this Review have analysed recent developments in several policy fields in relation to digitalisation in Latvia. The analysis led to an assessment of performance and a set of policy recommendations for each field. This section discusses these recommendations and maps them against the Going Digital Integrated Policy Framework presented in Chapter 1 and summarised in Figure 7.1.

The main components of the framework under analysis are **access**, **use**, **trust** and **innovation**. These were identified as priorities by the Latvian authorities. On their request, the Review also uses strategic foresight to examine key uncertainties surrounding the future of the digital transformation and the potential implications for Latvia.

Figure 7.1. Going Digital Integrated Policy Framework

Source: OECD (2019), *Going Digital: Shaping Policies, Improving Lives*, *https://doi.org/10.1787/9789264312012-en*.

Strategic foresight

The digital transformation is driving rapid change on an unprecedented global scale. At a time of rapid change and high uncertainty, strategic foresight intends to help Latvian decision makers better anticipate disruptive changes, identify critical uncertainties, develop innovative new strategies and policies, and stress-test existing plans and practices.

Strategic foresight begins by exploring a set of three scenarios. The first scenario considers a world where active citizens have taken digitalisation into their own hands and formed a comprehensive "third pillar" of online empowered communities that provide a counterweight to states and markets. The second scenario describes a world in which governments have set up digital platforms that become the backbone of their economies, and which promote exchange between countries using the same system but create barriers with those who do not. The third scenario presents a future in which multinational digital conglomerate corporations are able to serve their users so well that many of the roles traditionally held by the state, such as education and welfare, can be better offered by non-state entities.

These scenarios help to identify some key strategies for action for Latvia, which fall into four main categories:

- Evaluate and strengthen Latvia's strategic partnerships for digital transformation.
- Identify smart approaches to education and skills to produce more adaptive and critical Latvians.

- Identify pathways towards an inclusive digital Latvia by and for the people.
- Build capacity to benefit from access to and use of personal data, while safeguarding digital security and privacy.

Enhancing access and connectivity

Latvia is performing well in terms of deployment of both fixed and mobile broadband high-speed networks. In June 2019, mobile broadband subscriptions reached 127 subscriptions per 100 inhabitants, one of the highest rates among OECD countries. Fibre connections accounted for 70% of all fixed broadband connections, the fourth highest penetration in the OECD area after Korea, Japan and Lithuania. Prices for both fixed and mobile broadband connectivity are substantially lower than the OECD average.

Despite this performance, differences in connectivity persist between urban areas and rural areas, particularly when comparing Riga with other regions. There are also concerns about competition in the fixed broadband market, where the incumbent's share is 56%.

The recommended changes to policy design and regulatory frameworks listed below can help prepare Latvia to face coming developments in communication technologies and markets:

- Evaluate the benefits of creating a convergent regulator for both telecommunication and broadcasting services, particularly in relation to increasing the convergence of services over IP networks.
- Establish a clear ministerial focal point for communication services. Competencies are currently dispersed between the Ministry of Transport (MoT) and the Ministry of Environmental Protection and Regional Development (VARAM).
- Improve territorial planning in municipalities by promoting dig-once policies, granting permission for new towers, and planning new routes for fibre and cables, as well as harmonising and simplifying administrative procedures for network deployment.
- Increase co-ordination among municipalities and the MoT to overcome bottlenecks in fixed and mobile network deployment and prepare for network densification in line with the deployment of 5G.
- Reduce information asymmetries about available infrastructure and closely monitor for potentially discriminatory practices in access to passive infrastructure.
- Monitor the state of competition in the fixed broadband market and implement infrastructure-sharing obligations as appropriate.
- Engage with local stakeholders on last-mile solutions as part of rural broadband programmes and foster demand through targeted initiatives.
- Update the regulatory framework to allow for the development of a secondary spectrum market to promote more efficient usage.
- Develop and implement a national Internet of Things (IoT) plan to identify challenges and foster demand from businesses and consumers.
- Develop and implement a comprehensive IPv6 strategy in co-ordination with civil society, the private sector and technical stakeholders.
- Undertake an analysis of the state of traffic exchange and promote the deployment of neutral IXPs, based on good international practices.

Fostering effective use of digital technologies

Latvia has made significant progress in Internet usage in recent years, with the government becoming a leading user of digital technologies in Europe. Latvian people, however, remain moderate users of the Internet while businesses lag behind those in OECD countries. A large share of small firms and a lack of skills hold digital adoption back. Latvia also has the lowest employment share of ICT specialists – particularly women – in the European Union. The country should therefore implement a coherent set of measures to foster effective use of digital technologies by individuals, firms and government.

Upgrading digital skills

- Update training resources provided under the Third Father's Son programme, and provide libraries with sufficient resources to maintain ICT equipment.
- Create a community-based ICT training programme for groups with low digital uptake, similar to those in Australia and Norway.
- Support the development of modular programmes in higher education that include ICTs.
- Increase employer participation in defining university curricula, and introduce a legal framework for work-based learning in tertiary education.
- Strengthen links between vocational schools and firms employing ICT specialists, and simplify procedures to grant firms support for on-the-job training.
- Introduce training vouchers for employees funded out of an employers' contribution on gross wages, as used in France and Poland.
- Exempt foreign ICT specialists with proven experience, or who completed their studies in Latvia, from labour market tests, as is the case in Germany and the United Kingdom.

Increasing digital uptake by firms

- Create a digital champions programme, like the one in Australia, whereby the government provides support to a small number of SMEs in sectors with low ICT uptake.
- Provide consultancy and management advice to help firms catch up with highly digitised firms, as already done in Australia and Austria.
- Introduce a system that enables business payroll software to automatically report data to tax authorities, similar to Australia's Single Touch Payroll system.

Fostering digital government

- Consolidate funding for digital government into a single ministry, which can then set priorities in accordance with a national strategy.
- Create a civil service-wide training programme on the use of ICTs and the design of e-government services, and develop a manual of good practices, like that in the United Kingdom.
- Introduce incentives for businesses to interact with government online (e.g. to issue permits or payments more quickly than offline operations). Set a schedule for phasing out selected e-government services offline.
- Develop new rules, procedures and standards on the use of telemedicine, like the Act on eHealth and Secure Data Sharing in the Czech Republic.
- Establish a one-stop shop for those who wish to access health and social care data for research, such as in Finland.
- Promote an open data ecosystem by granting prizes to tertiary-level students and researchers making use of open data to address societal challenges.

Enhancing trust in a digital environment

Fostering digital security

Latvia has built solid foundations from which to address the challenges and opportunities of digital security. The Latvian Computer Emergency Response Team (CERT.LV) is recognised internationally for its technical expertise and vulnerability disclosure policies. The Latvian Ministry of Defence (MoD) is also strongly committed to promoting digital security as a strategic issue, as showed in the recently adopted *Cyber Security Strategy (2019-2022)*. The creation in 2011 of the Latvian National Information Technology Security Council (NITSC) represents a further step in developing a whole-of-government approach to digital security.

However, digital security policy in Latvia is still narrowly focused on national security, with insufficient attention paid to the economic and social dimensions of digital security.

To tackle these issues, Latvia should:

- Promote the digital security strategy at the highest level of government.
- Step up the involvement of ministries with a cross-cutting mandate (e.g. those in charge of economic and regional development) in digital security initiatives.
- Better integrate the digital security strategy with the Information Society Development Guidelines.
- Promote upskilling and workforce-sharing programmes between public institutions.
- Increase multi-stakeholder co-operation on digital security policy making through trust-based partnerships.
- Enhance international co-operation in the area of digital security for economic and social prosperity, in particular with other Baltic countries.

Enhancing privacy

Latvia has made significant progress in enforcing the privacy and data protection rights of individuals since the enactment of the EU General Data Protection Regulation (GDPR) and the Personal Data Processing Law (PDPL) in 2018. The Data State Inspectorate (DSI) has begun enforcing both legal frameworks in a proactive fashion and has levied administrative fines against companies for non-compliance with the general obligations in both laws.

Latvia should take the following further steps to enhance privacy:

- Provide the DSI with the human and financial resources necessary to perform its tasks effectively, including by advising and investigating privacy and data protection in the digital space.
- Develop DSI guidance on privacy and privacy management programmes (PMPs), based on existing good international practice.
- Encourage co-operation between the DSI and other countries, including outside the European Union, for example, by joining the Global Privacy Enforcement Network (GPEN).
- Establish appropriate data governance of artificial intelligence (AI) and the IoT, including through further participation and collaboration with international fora such as the OECD.

Enhancing consumer protection online

Latvia's consumer policy framework incorporates general principles for protecting digital consumers consistent with the OECD *Recommendation of the Council on Consumer Protection in E-commerce* (OECD, 2016). However, the government could act to improve its evidence base for consumer policy decision making, and enhance consumer protection within and outside the European Union, as follows:

- Collect and analyse consumer complaints data specific to e-commerce in order to better understand the nature and scale of consumer issues associated with e-commerce transactions.
- Enhance consumer awareness of issues associated with e-commerce, targeting the special needs of different groups based on their age, income and literacy.
- Assess the effectiveness of the dispute resolution and redress system, by exploring consumer usage and satisfaction, and analysing unresolved dispute cases.
- Improve the evidence base on cross-border disputes outside the European Union and enhance cross-border enforcement co-operation within and outside the European Union.

Unleashing digital innovation

Latvia has made significant economic progress since the beginning of the millennium. The economy has grown faster than in any other EU and OECD countries. Latvia's National Research and Innovation Strategy for Smart Specialisation (RIS3) aims to promote structural transformation of the economy towards knowledge-based activities. Productivity, however, remains significantly lower than in other OECD countries, while a declining working age population limits the prospect for further growth. Innovation is therefore key to increasing productivity and raising living standards in Latvia.

In order to increase research and development (R&D) and foster innovation in businesses, Latvia should:

- Focus on digitalisation as a key transversal enabler of innovation and growth.
- Promote digital service innovation.
- Promote digital innovation to address Latvia's societal and economic challenges.
- Increase the level of public support to business R&D and diversify its composition towards greater use of tax allowance for R&D expenditures.
- Allocate a greater proportion of research funding to ICT-related projects, which are currently underfunded.
- Increase the share of RIS3 funding devoted to ICTs and target applications of high relevance for other Smart Specialisation areas.
- Raise the quality of research by increasing the proportion of funding allocated through a competitive process.
- Introduce a system of *ex post* evaluation of research projects, similar to Science Foundation Ireland.
- Raise the proportion of private co-financing of competence centres to ensure they are geared towards commercial innovations.
- Assess the activities of the IT Cluster, LIKTA, LIDA and the IT Competence Centre and clearly define their respective roles based on this assessment.
- Develop an intellectual property rights (IPRs) strategy, based on the successful example of Finland, and establish a specialised court for all IPR issues.
- Raise business incentives to invest in R&D by making existing tax incentives for R&D staff in start-ups less generous but available to all firms.

Building a whole-of-government approach for digital transformation policy

The digital transformation affects different parts of the economy and society in complex and interrelated ways, making trade-offs between public policy objectives difficult to navigate. Leveraging the benefits and addressing the challenges of digital transformation requires co-ordination across all policy domains identified in the Going Digital Integrated Policy Framework (Figure 7.1). It also requires the consideration of transversal policy issues (e.g. skills, digital government and data governance) that cut across several of the framework's policy dimensions (OECD, 2019). The above policy recommendations, therefore, need to be co-ordinated through a whole-of-government approach.

Co-ordination implies the involvement of a wide range of actors across multiple parts and levels of government, as well the participation of non-governmental stakeholders and international partners. A whole-of-government approach, however, may prove challenging. For example, high transaction costs, power and information asymmetries, and different governance approaches across different levels of government can make co-ordination and negotiations cumbersome.

While well-designed governance is fundamental to effective co-ordination. However, there is no one-size-fits-all approach. Different approaches can reflect, for example, variations in state institutions, the organisation of government, or administrative culture and capacity. In addition, governance arrangements are likely to evolve over time, for example with changes in government, technological progress and shifts in the constellation of actors driving digital transformation.

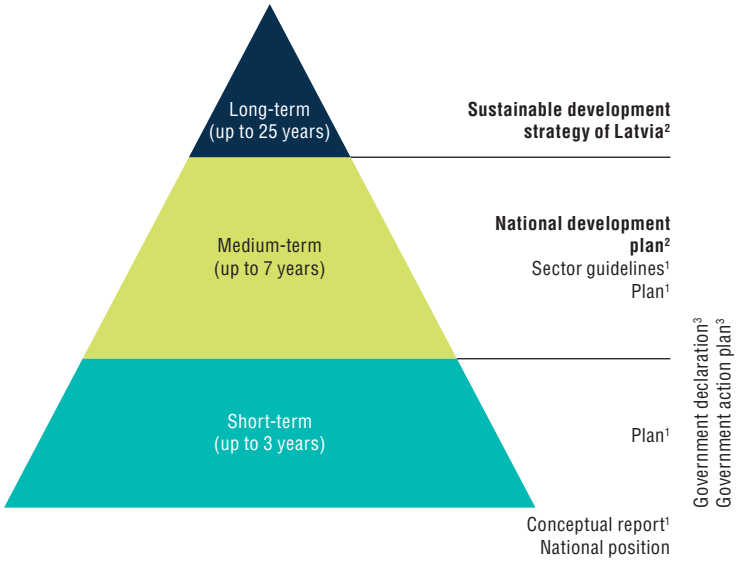
This section examines the current co-ordination mechanism of policies for digital transformation in Latvia and makes recommendations to help ensure a coherent and cohesive whole-of-government approach to policies for digital transformation.

Latvia's Sustainable Strategy 2030

Latvia has a hierarchical policy planning system with long-term (up to 25 years), medium-term (up to seven years) and short-term (up to three years) horizons (Figure 7.2). The Sustainable Development Strategy is the highest national-level, long-term planning document. It sets the main priorities for the government and society in order to achieve balanced and sustainable development.

Latvia 2030, the current Sustainable Development Strategy, includes 7 development priorities, 7 strategic indicators, 11 objectives, 11 development directions, 42 areas of action and 27 performance indicators (SAEIMA, 2010).

Figure 7.2. Latvia's national development planning



1. Policy planning document.
2. Spatial planning document.
3. Political guidance document.

Source: CSCC (2012), *National Development Plan of Latvia 2014–2020*, *www.pkc.gov.lv/index.php/en/national-development-planning/national-development-planning*.

Latvia 2030 considers digitalisation in relation to national development priorities. Development of the cultural space (priority 1) regards digital technologies as an opportunity to improve access to culture, preserve Latvia's language and cultural heritage. and strengthen national identity. The Sustainable Development Strategy allots libraries the role of local competence centres geared towards providing life-long education and information to foster long-term investments in human capital (priority 2).

Digitalisation is also expected to contribute to changing the education paradigm (priority 3), through improved access to networks of social services, the digitisation of schools, libraries and educational material, and e-learning.

Open knowledge and science, through virtual business incubators, digital networks and platforms, have the potential to promote an innovative and eco-efficient economy (priority 4). Digital licensing is expected to ease access to intellectual property and reduce licensing costs. A shift away from using transport towards teleworking and distant learning would also reduce energy consumption and gas emissions.

Digital technologies and platforms can help establish natural assets as future capital (priority 5) and stir and diffuse new practices to reduce the ecological footprint of human activities. The deployment of high-speed broadband networks would make advanced digital services available in rural areas and remote regions, thus enhancing regional development (priority 6).

Finally, digitalisation is regarded as a means to enhance government innovation and public participation (priority 7). E-government has the potential to deliver better services in a more efficient way, while social networks and Internet platforms can act as public fora where citizens can share opinions and collaborate to address societal challenges.

Latvia 2030 also identifies 27 indicators to measure progress across the 7 development priorities. However, only one indicator (i.e. use of e-government by individuals, has a direct link to digital transformation).

As a high-level policy document, Latvia 2030 does not detail specific actions; these are developed and detailed in national plans and sectoral guidelines.

The National Development Plan 2014-2020

The main tool for the implementation of the Sustainable Development Strategy is the National Development Plan (NDP), Latvia's main medium-term development planning document. The NDP set outs the main medium-term objectives, priorities and performance indicators, areas of action, outcomes and responsible institutions for a period of seven years. The plan is implemented via the development policies of sectors and territories (regions, local governments), including through the planning investment programmes of central and local governments, EU policy instruments and other financial sources.

The NDP 2014-2020 sets out 12 strategic objectives under three priorities: 1) growth of the national economy; 2) human security; and 3) growth for regions (CSCC, 2012). Several actions foreseen in the NDP leverage digital transformation to achieve strategic objectives, as discussed above.

To achieve the strategic objective "Highly productive manufacturing and internationally competitive services with export potential", the NDP foresees training for entrepreneurs in productivity-enhancing production processes, and management methods and business models, including those enabled by digital technologies.

Actions to attain the strategic objective "Services for more equal work opportunities and living conditions" include enhanced access to high-speed and ultra-high-speed data transmission networks throughout Latvia, general improvement of e-skills among the population and enhanced access to e-government services, and the development of digital content, products and services.

To achieve the strategic objective "Development of competencies", the NDP foresees the introduction of innovative forms of content and activities in elementary and secondary education to promote creative and entrepreneurial skills in a digital learning environment.

Reduction of the administrative burden on businesses, including through digital technologies, and the establishment of a one-stop online platform for e-government services to businesses, form part of the actions to achieve the strategic objective to create "(a)n outstanding business environment".

Finally, achievement of the strategic objective "Advanced research and innovation and higher education" is reliant on the establishment and development of a co-operation platform for higher education, science and the private sector among Baltic countries, in selected areas, including smart technologies and engineering. The NDP encompasses other actions to support research and technological transfer, but does not refer specifically to digital technologies.

The NDP does make specific reference a set of indicators to assess progress. While several indicators are likely to include a digital component (e.g. R&D, high-tech exports and skills), only two incorporate a direct link to digital transformation: 1) the proportion of households with access to the Internet; and 2) the proportion of the population who use the Internet to interact with state and local government institutions. The 2020 targets for both indicators – 80% and 60%, respectively – have been achieved (Chapter 4).

The NDP for the period 2021-27 was approved by the Cabinet of Ministers on 25 February 2020. The NDP 2021-2027 establishes three strategic goals – equal opportunity, productivity and income, and social trust – for six priority areas: 1) strong families, healthy and active people; 2) knowledge and skills for personal and national growth; 3) competitiveness of business and material well-being; 4) quality living conditions and territorial development; 5) culture and sports for active and fulfilling life; and 6) a united, secure and open society.

The NDP 2021-2027 includes several measures leveraging digital opportunities:

- strengthening digital and new technology skills in co-operation with businesses
- promoting the use of digital technologies in business

- furthering the diffusion of digital solutions for the exchange of information among economic operators, national and local authorities
- mainstreaming the "go digital first" principle for user-oriented, open public services
- enhancing ICT infrastructure for public administration, municipalities and education institutions
- increasing physical and digital accessibility to national and municipal infrastructure
- promoting Smart Specialisation Strategies in five areas, including ICTs
- preserving and transmitting cultural heritage, sport traditions and values to future generations, including through ICTs.

The Information Society Development Guidelines 2014-2020

The Information Society Development Guidelines (INFSO) 2014-2020 – next in Latvia's hierarchical policy planning system – lay down the digital strategy (Cabinet of Ministers, 2013a). The Guidelines function as a medium-term development plan and were developed by a working group co-ordinated by the Ministry of Environmental Protection and Regional Development (VARAM) and composed of representatives from 12 ministries (Agriculture, Culture, Defence, Economy, Education, Finance, Foreign Affairs, Health, Interior, Justice, Transport and Welfare), the State Chancellery, ICT industry associations, the Latvian National Commission for UNESCO and the Latvian Chamber of Commerce.

The aim of INFSO 2014-2020 is "to provide an opportunity for everyone to use the possibilities offered by ICTs, to develop a knowledge-based economy and to improve the overall quality of life by contributing to national competitiveness, and increasing and economic growth and job creation" (Cabinet of Ministers, 2013a).

Economic growth and job creation are at the core of the strategy and inform the formulation of each of the seven Action Directions put forward in the Guidelines: 1) ICT education and skills; 2) widely available access to the Internet; 3) advanced and effective public administration; 4) e-services and digital content for the public; 5) cross-border co-operation for digital single market; 6) ICT research and innovation; and 7) trust and security.

The Guidelines devote particular attention to the use of open data principles in public administration as a tool to improve efficiency in public service delivery. Upgrading e-skills and improving Internet access and speed also have a prominent role, as enablers for e-commerce and e-business more. Using digital tools to reduce the administrative burden and improve the efficiency of the public administration is also key to the INFSO 2014-2020, with a view to reducing administrative costs for businesses, especially SMEs.

Each Action direction is articulated along several measures, as shown in Table 7.1.

An interim assessment of implementation of the guidelines was completed in October 2019 (VARAM, 2019). The final assessment will be submitted by VARAM to the Cabinet of Ministers in July 2021.

The INFSO interim assessment concludes that human capital and innovation, together with interoperability of digital solutions, are key for the digital transformation. In order to gain synergies between the public administration and the private sector should be further developed, by improving the existing institutional framework and developing a new framework that responds to the challenges posed by digitalisation.

Several other development documents are currently in force, often with a focus on improving e-government services. These include the *Concept of the Organisational Model of Public ICT Management* (Cabinet of Ministers, 2013b), the *Conceptual Architecture of Public Administration Information Systems* (Cabinet of Ministers, 2015), the information reports *Using Cloud Computing Services in Public Administration* (Cabinet of Ministers, 2018) and *Latvia's Open Data Strategy* (Cabinet of Ministers, 2019) (Chapter 4) as well as the informative report on *Artificial Intelligence Solutions* (Cabinet of Ministers, 2020a) and the *Public Services Transformation Action Plan* (Cabinet of Ministers, 2020b).

Table 7.1. Information Society Development Guidelines 2014-2020

Action direction	ICT in education and e-skills		
Key measures	**Responsible institution**	**Institutions involved**	**Planned expenditure (LVL)**
1.1 E-skills upgrade of employees and entrepreneurs	VARAM	Local governments, all ministries	4 035 294
1.2 Training of employees in partnership with businesses	MoE	LIDA	15 000 000[1]
1.3 E-skills training for the unemployed and job seekers	MoW	MoE, MoES, local governments, SEA, social partners	10 000 000
1.4 E-skills training for adults	MoW	MoE, MoES, social partners	1 900 000
1.5 Digital textbooks library	MoES	MoC, VARAM, municipalities, NCE, social partners	694 118
1.6 Development of an integrated education curriculum, including algorithmic thinking and information literacy	MoES	SECC, MoC, VARAM, municipalities, social partners	1 058 824[1]
1.7 Digital learning materials for general education	MoES	MoC, VARAM, municipalities, social partners	2 966 667
1.8 Natural sciences cabinet equipment in schools, including software	MoES	Municipalities	18 000 000[1]
1.9 Methodological support in ICTs	MoES	Municipal and state grammar school	10 000 000
1.10 Ergonomic arrangements and innovative ICT solutions in regional secondary schools	MoES	Municipalities	57 400 000
1.11 Qualification upgrade of teachers, including in ICTs	MoES	SECC, municipalities	6 000 000[1]
1.12 Skills upgrade of teachers, including ICT skills	MoES	Municipalities, MoA, MoC, MoE, MoW, social partners	3 507 100
1.13 Management improvement in small rural schools, including through ICT acquisition	MoES	Municipalities	11 764 706
1.14 Development of a next-generation network in rural areas	MoT	State Radio and Television Centre	65 000 000
1.15 Broadband for the last mile of connection	MoT	Telecom companies	36 000 000
1.16 Evaluation of existing electronic communications grids	MoT	..	MoT regular budget
1.17 Mapping of the current electronic communications network infrastructure	MoT	..	2 400 000
3.1 Development of ICT centralised platforms for the public administration	VARAM	All ministries	25 035 294
3.2 Digitalisation of public administration services	VARAM	All ministries, local governments	76 258 824
3.3 Introduction of the state administration human resource management system based on e-government principles	SAO	Public Administration School, all ministries	6 670 600[1]
3.4 Introduction of e-auctions	MoJ	CA, IAC	1 000 000
3.5 Development of a single IT platform for patent, trademark and design registration	MoJ	Patent office	800 000
3.6 Introduction of the labour market forecasting system	MoW	MoE, MoES, MoW, social partners	764 706
3.7 Higher efficiency of inpatient health care institutions	MoH	Local governments, social partners	3 000 000
3.8 Quality improvement of disability expertise services	MoW	MoH municipalities, social partners	505 882
3.9 Online psychological consultations for children in distress	MoW	SIPCR	120 000
3.10 Engagement with civil society on web 2.0 solutions	SAO	All ministries, social partners	300 000
3.11 Development of a research and publication database	CSCC	..	11 800
3.12 Development of an integrated database on climate change and air quality	VARAM	IPE, LEGMC, LUA, Silava	In budget
3.13 Assessment of climate change reduction policy	VARAM	IPE, LEGMC, LUA, Silava	In budget
3.14 Development of climate change portal	VARAM	..	In budget
3.15 Development of an information system on flood risk areas	VARAM	..	In budget
3.16 E-services and systems related to law	MoJ	CA (LR), DSI, IAC, RE, SFSB, SLS,	7 000 000
3.17 Digitisation of cultural heritage	MoC	CISC, LNB, MoC	11 764 706
3.18 Update of library, archive and museum information system in accordance with EU Directive 2013/37/EU	MoC	CISC, LNB, MoC	1 750 000
3.19 Development and maintenance of the digital cultural heritage competence network	MoC	CISC, LNB, MoC	3 000 000

Table 7.1. Information Society Development Guidelines 2014-2020 *(cont.)*

Action direction	ICT in education and e-skills		
Key measures	**Responsible institution**	**Institutions involved**	**Planned expenditure (LVL)**
3.20 Improvement of the machine translation system	MoC	CISC	4 000 000
3.21 Development of ICT management system for central government	VARAM	SRDA	1 487 022
6.1 Support to applied R&D for commercial use	MoES	MoA, MoC, MoE, VARAM, MoH, Registered Scientific Institutions	32 500 00[1]
6.2 Support for new products and technologies	MoE	LIDA	124 000 000[1]
7.1 Development of the Latvian centralised ICT security and prevention platform	CERT.LV/MoD	National regulatory authorities	515 530
7.2 Electronic reporting of illegal and harmful content on the Internet	CERT.LV/MoD	LIA	184 200
7.3 Public awareness raising on ICT security	VARAM	CERT.LV, MoD	4 035 294
7.4 Public awareness raising on risks and threats on the Internet	VARAM	CERT. LV/MoD, LIA, MoW, SIPCR	208 200
7.5 Helpline for children and youth affected by harmful content on the Internet	MoW	SIPCR	220 200
7.6 Public awareness raising about personal data security	MoJ	CERT.LV, DSI, VARAM	53 400
7.7 Informing State administrative institutions about the necessity to ensure personal data processing safety in the Internet environment	MoJ	CERT.LV, DSI, VARAM	12 000
7.8 Securing a high level of protection of activities dealing with personal data	DSI	..	629 778
7.9 Modernisation of the 112 call platform	MoI	VARAM	8 800 000

1. Only some of the expenditure relates to the INFSO 2014-2020 measures.

Notes: .. = not available. The Latvian latz (LVL) was replaced by the euro on 1 January 2014, 1 LVL = EUR 1.42288. CA = Court Administration; CERT.LV = Computer Emergency Response Team of Latvia; CISC = Cultural Information System Centre: CSCC = Cross-Sectoral Coordination Centre; DSI = Data State Inspectorate; IAC = Internal Audit Council; IPE = Institute of Physical Energetics; LEGMC = Latvian Environment, Geology and Meteorology Centre; LIA = Latvian Internet Association; LIDA = Latvian Investment and Development Agency; LNB = Latvian National Library; LR = Land Registry; LUA = Latvian University of Agriculture; MoA = Ministry of Agriculture; MoC = Ministry of Culture; MoD = Ministry of Defence; MoE = Ministry of Economy; MoES = Ministry of Education and Science; MoH = Ministry of Health; MoI = Ministry of Interior; MoJ = Ministry of Justice; MoT = Ministry of Transport; MoW = Ministry of Welfare; NEC = National Centre for Education; RE = Register of Enterprises of the Republic of Latvia; SAO = State Audit Office; SFSB = State Forensic Science Bureau; Silava = State Forest Research Institute; SIPCR = State Inspectorate for Protection of Children's Rights; SLS = State Land Service; SRDA = State Regional Development Agency; VARAM = Ministry of Environmental Protection and Regional Development.

Source: Cabinet of Ministers (2013a), *Information Society Development Guidelines 2014-2020 – Informative Part, Order No. 486, 14 October*, *www.varam.gov.lv/in_site/tools/download.php?file=files/text/Darb_jomas/elietas//Information_Society_Development_Guidelines_2014_2020.docx*.

Other documents, such as the Concept for the Development of Next Generation Broadband Electronic Communications Networks 2013-2020 and the Electronic Communications Policy Plan 2018-2020, focus more on ICT access and infrastructure (Chapter 3).

Additional documents include the Guidelines for the Protection and Enforcement of Intellectual Property Rights 2015-2020 and the Cyber Security Strategy of Latvia (2014-2020). The Guidelines for the Cyber Security Strategy of Latvia (2019-2022) were approved in September 2019 (Chapter 5).

Latvia does not currently have an overarching strategy in place for the digitalisation of business. There is, however, a Smart Specialisation Strategy, which is flanked by the *Science, Technological Development and Innovation Guidelines for 2014-2020* (STDI) and the *National Industrial Policy* (NPI) guidelines for 2014-2020. The latter aim explicitly at promoting the modernisation of industry. The NPI guidelines were published in 2012 and aim, among other objectives, to align labour supply and education to the needs of economic development, and to promote open, creative and innovative environments (Chapter 6).

Clear budgetary appropriations for the digital strategy

The INFSO 2014-2020 includes information on the expenditure required for implementation (Table 7.1), but does not provide for any budgetary appropriation. The Guidelines, therefore, must be implemented from the regular budget of each ministry. This leaves significant discretionary power in the hands of

the ministries regarding the resources devoted to measures foreseen under the Guidelines and their actual implementation.

Furthermore, the lack of a specific budget for the INFSO 2014-2020 makes it difficult to assess the actual allocation of resources *ex post*. This difficulty is illustrated by the INFSO progress assessment carried out in 2019, which does not report any information on actual expenditures by responsible ministries for measures foreseen under the Guidelines.

Similarly, it is difficult to identify resources allocated for implementation of the Guidelines in the central government budget. For instance, under the INFSO 2014-2020, the Ministry of Economy (MoE) should allocate a proportion of its 2014-20 budget for the training of employees (EUR 10.5 million) and provide support for new products and technologies (EUR 87.1 million) related to digital uptake and skills. In the MoE budget, these measures are listed mainly under the European Regional Development Fund (ERDF), which has an overall budget of less than EUR 50 million for 2018-20. In addition, the actual level of resources allocated to policies for digital uptake and skills is not reported.

Similarly, EUR 40.3 million should be devoted to the measure "Ergonomic arrangements and innovative ICT solutions in regional secondary schools", one of the largest planned expenditures in the Guidelines. While local governments were designated to implement 44 projects as part of this measure, expenditures for ICT solutions (EUR 23 million) seem significantly below the level planned in the INFSO 2014-2020.

The large number of sectoral guidelines developed in Latvia appear to constitute an obstacle to clear alignment between policy initiatives and budget appropriations. Although these guidelines favour co-operation among ministries and agencies in specific policy fields, their volume leads to some overlap of measures across several guidelines.

Furthermore, while the ministries responsible for each set of guidelines are accountable for their implementation, line ministries seem to enjoy weaker accountability, reducing their incentives to implement the guidelines (OECD, 2018). This helps to explain why Latvia has made more progress on measures related to e-government, as VARAM is responsible for both the INFSO 2014-2020 Guidelines and e-government policies.

These issues are acknowledged in Latvia 2030: "A large number – several hundred – of development planning documents … have been created. The development planning system is poorly connected with the budgetary process and lacks medium-term and long-term assessment ... The strong sectoral perspective in the design and implementation of policies … is a further source of difficulties". The Sustainable Development Strategy was meant to be a single instrument, which together with a change in governance model would address these issues. However, formal respect for the objectives set in the Sustainable Development Strategy and the NDPs aside, persistent tension among sectoral guidelines remains a strong obstacle to policy making in Latvia.

Stronger co-ordination mechanisms within government

Three steps seem necessary to increase government commitment to the digital agenda. The first is to push digital transformation policies higher up the policy agenda. This means that digital transformation objectives should have a more prominent role in the Sustainable Development Strategy and National Development Plans. As discussed above, these documents foresee policies for the digital transformation but do not provide sufficient detail about their nature and scope. While a new NDP is being developed for the period 2021-27 with the option to strengthen the role of digital transformation policies, the Sustainable Development Strategy will be in place until 2030. Therefore, the government should explore the opportunity to revise the strategy with a view to providing a stronger and clearer commitment to digital transformation policies.

The second step is to define clear budget appropriations for the Information Society Development Guidelines for the next planning period. While it seems appropriate to leave the implementation of these guidelines to each ministry, which will have better information regarding its sector of competency, it is necessary to set clearer budgetary appropriations and clearer spending commitments at the ministerial level. This would increase transparency regarding the objectives of the Guidelines, send a strong signal confirming the government's commitment and strengthen the political credibility of the measures. More transparency would also facilitate implementation of the Guidelines.

Finally, it is important to establish some institutionalised mechanisms for co-ordinating digital transformation policies across the government. Leadership, design and management of the Information Society Development Guidelines are spread among several ministries, including VARAM, the MoE, the MoT and the MoES. The lack of a formal, whole-of-government approach hampers the overall effectiveness of Latvia's digital transformation agenda.

The INFSO 2014-2020 progress assessment reaches a similar conclusion, calling for balanced integration of digitalisation policy into sectoral policies, with sufficient resources for policy co-ordination, adequate funding to achieve the objectives pursued and ambitious but achievable indicators.

OECD countries employ different governance models for their national digital strategies (Table 7.2). Some rely on a dedicated ministry or body; others incorporate co-ordination of the national digital strategy into the portfolio of a minister or body. In a few, co-ordination is the responsibility of several ministries or is taken up at the highest level of government (i.e. Prime Minister's Office, Presidency or Chancellery).

Table 7.2. Governance of national digital strategies in OECD countries

Number of countries

Responsible body	Co-ordination	Implementation	Monitoring	Evaluation
Prime Minister's Office, Presidency or Chancellery	5	0	3	4
Dedicated ministry or body	12	8	12	10
Non-dedicated ministry or body	14	4	12	11
Several ministries or bodies	6	24	8	8

Note: The data are based on survey responses from 33 countries. The sum of each responsibility may exceed the number of countries (33) when responsibilities have been assigned to more than one body.

Source: OECD (2019), *Going Digital: Shaping Policies, Improving Lives*, *https://doi.org/10.1787/9789264312012-en*.

While the above models all have strengths and weaknesses, it is essential that the body responsible for the co-ordination of the digital strategy have both sufficient political leverage and adequate resources to fulfil its mandate.

The Deputy Prime Minister appears to be a natural candidate for the co-ordination of digital transformation policies in Latvia. Appointed by the Cabinet, the Deputy Prime Minister is responsible for the government's National Development Plan and its coherence with the Sustainable Development Strategy as well as with the budgetary process. In this function, she or he can help ensure that digital transformation policies are placed at the highest level of the policy agenda.

The role of co-ordinating the digital economy strategy could be supported by the Cross-Sectoral Coordination Centre (CSCC). The CSCC is the leading institution on national development planning and co-ordination in Latvia. Placed under the direct authority of the Prime Minister, the CSCC is responsible for developing and monitoring the Sustainable Development Strategy and the National Development Plan. It also performs analytical tasks assigned by the Prime Minister and the Prime Minister's Office, including assisting with the Government Declaration and Action Plan.

As the co-ordinator of Latvia's digital economy strategy, the Deputy Prime Minister should also have a discretionary budget that can be used to co-finance policies, according to objectives set by the government, implemented in co-ordination with two or more institutions: ministries, agencies or local governments. While line ministers would retain the responsibility and appropriations to implement digital transformation policies in their field, this budget would provide an incentive for institutional co-operation. For instance, the Deputy Prime Minister could allocate an additional allocation (i.e. a kind of co-ordination premium) for policies implemented through co-ordination among several ministries.

These budgetary allocations would typically take the form of a matching grant, (i.e. a grant that must be used for a specific purpose and is conditional on additional resources from the receiving institutions).

The budget would not require additional resources but a reallocation of the appropriations currently allocated to digitalisation policies under different lines of the central government budget. A clearer budgetary allocation, as discussed above, is a prerequisite for the establishment of this co-ordination mechanism.

Box 7.1. Policy recommendations for a whole-of-government approach

To help ensure a coherent and cohesive whole-of-government approach to digital transformation policies in Latvia, the government should:

- Push digital transformation policies higher up the policy agenda
- Define clear budget appropriations for the Information Society Development Guidelines
- Institutionalise a co-ordination mechanism for digital transformation policies (e.g. by investing the Deputy Prime Minister with the role of co-ordinator).

References

Cabinet of Ministers (2020a), *Informatīvais ziņojums "Par mākslīgā intelekta risinājumu attīstību"* [Developing Artificial Intelligence Solutions], Riga, *http://tap.mk.gov.lv/doc/2020_02/IZ_MI%5b1%5d.2.docx*.

Cabinet of Ministers (2020b), *Public Services Transformation Action Plan*, Riga.

Cabinet of Ministers (2019), *Latvijas atvērto datu stratēģija* [Latvia's Open Data Strategy], 20 August, Riga, *http://polsis.mk.gov.lv/documents/6533*.

Cabinet of Ministers (2018), *Informatīvais ziņojums "Mākoņdatošanas pakalpojumu izmantošana valsts pārvaldē"* [Using Cloud Computing Services in Public Administration], 20 February, Riga, *http://polsis.mk.gov.lv/documents/6140*.

Cabinet of Ministers (2015), *Conceptual Architecture of Public Administration Information Systems*, 10 March, Riga.

Cabinet of Ministers (2013a), *Information Society Development Guidelines 2014-2020 – Informative Part*, Order No. 486, 14 October, Riga, *www.varam.gov.lv/in_site/tools/download.php?file=files/text/Darb_jomas/elietas//Information_Society_Development_Guidelines_2014_2020.docx*.

Cabinet of Ministers (2013b), *Concept of the Organisational Model of Public ICT Management*, Order No. 57, 15 January, Riga, *www.varam.gov.lv/in_site/tools/download.php?file=files/text/Darb_jomas/elietas//E2269_Organisational_Model_for_the_Management_of_Public_Infor_and_Com_Techn.doc*.

CSCC (2012), *National Development Plan of Latvia 2014–2020*, Cross-Sectoral Coordination Centre, Riga, *www.pkc.gov.lv/images/NAP2020%20dokumenti/NDP2020_English_Final.pdf*.

OECD (2019), *Going Digital: Shaping Policies, Improving Lives*, OECD Publishing, Paris, *https://doi.org/10.1787/9789264312012-en*.

OECD (2018), *Access to Justice for Business and Inclusive Growth in Latvia*, OECD Publishing, Paris, *https://doi.org/10.1787/9789264303416-en*.

OECD (2016), *Consumer Protection in E-commerce: OECD Recommendation*, OECD, Paris, *www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf*.

SAEIMA (2010), *Sustainable Development Strategy of Latvia until 2030*, Riga, *www.varam.gov.lv/in_site/tools/download.php?file=files/text/dokumenti/pol_doc//LIAS_2030_parluks_en.pdf*.

VARAM (2019), *2nd Interim Evaluation of the Information Society Development Guidelines 2014-2020*, Ministry of Environmental Protection and Regional Development, Riga, *http://polsis.mk.gov.lv/api/file/file7299860066764117769.pdf*.

List of Figures

List of Tables

List of Boxes

OECD Reviews of Digital Transformation

Going Digital in Latvia

Going Digital in Latvia analyses recent developments in Latvia's digital economy, reviews policies related to digitalisation and make recommendations to increase policy coherence in this area, based on the OECD Going Digital Integrated Policy Framework.

The review uses strategic foresight to explore three alternative future scenarios, which could result from the digital transformation of the global economy and society. It also examines the availability and quality of communication networks and services in Latvia as well as related policies and regulations. Further, it reviews trends in digital technology usage among individuals, businesses and the government, and examines policies to foster diffusion. Finally, the review analyses opportunities and challenges raised by digitalisation in key areas, from innovation and skills to digital security and data governance, and evaluates policy responses to these changes in Latvia.

This publication is a contribution to the OECD Going Digital project which aims to provide policymakers with the tools they need to help their economies and societies prosper in an increasingly digital and data-driven world.

For more information, visit ***www.oecd.org/going-digital***

#GoingDigital

PRINT ISBN 978-92-64-55190-9
PDF ISBN 978-92-64-83854-3