

PROMOTING COMPARABILITY IN PERSONAL DATA BREACH NOTIFICATION REPORTING

OECD DIGITAL ECONOMY
PAPERS

December 2021 **No. 322**

Foreword

This report aims to help improve the comparability of personal data breach notification reporting in response to the call at the 2016 Cancun Ministerial Meeting for better metrics on privacy and security in the digital economy. It analyses the main findings of the June 2019 to February 2020 survey, which identifies a core set of questions suitable for internationally comparable data collections by privacy enforcement authorities. The report also sheds light on the policy environment and actions necessary for improving international comparability.

This report was drafted by Suguru Iwaya, Elif Koksal-Oudot and Elettra Ronchi from the OECD Secretariat under the supervision of Elettra Ronchi.

It benefitted from the input of delegates of the Working Party on Data Governance and Privacy (DGP) and the Working Party on Measurement and Analysis of the Digital Economy (MADE). The authors gratefully acknowledge support of the Global Privacy Assembly, the Asia Pacific Privacy Authorities, the US Federal Trade Commission and the European Data Protection Board in the distribution of the questionnaires and for the valuable feedback received at each stage. The Secretariat wishes to thank Barbara Bucknell (Canada), Guilherme Roschke (United States) and Gwendal Le Grand (France) for their guidance and assistance in the interpretation of results.

This paper was approved and declassified by written procedure by the Committee on Digital Economy Policy (CDEP) on 31 August 2021 and prepared for publication by the OECD Secretariat. This publication is a contribution to IOR to 01471-131-1.3.1.1.3 of the CDEP's 2019-20 Programme of Work and Budget.

Note to Delegations:

This document is also available on O.N.E under the reference code:

DSTI/CDEP/DGP(2020)1/FINAL

This document, as well as any data and any 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.

© OECD 2021

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

Table of contents

| | |
|--|-----------|
| Foreword | 2 |
| Executive summary | 6 |
| Introduction | 9 |
| Analysis of the responses | 10 |
| <i>A. Authority profiles</i> | 10 |
| <i>B. Authority's funding and resources</i> | 12 |
| <i>C. PDBN reporting law, jurisdiction and exemptions</i> | 16 |
| <i>D. Personal data breach annual reporting</i> | 23 |
| <i>E. Number of personal data breach notifications received</i> | 25 |
| <i>F. Personal data breach notification by sector</i> | 29 |
| <i>G. Nature and type of personal data breach incident</i> | 32 |
| <i>H. Types of personal data affected</i> | 35 |
| <i>I. Monetary fines and other penalties</i> | 36 |
| <i>J. Measures taken to prevent or mitigate risk and evaluating PDBN impacts</i> | 39 |
| <i>K. Use of PDBN data</i> | 42 |
| <i>L. Summary of potentially workable questions</i> | 45 |
| ANNEX A. Revised questionnaire | 47 |
| <i>A. General questions and authority profile</i> | 47 |
| <i>B. Authority's funding and human resources</i> | 48 |
| <i>C. Personal data breach notification reporting law, jurisdiction and exemptions</i> | 51 |
| <i>D. Personal data breach annual reporting</i> | 57 |
| <i>E. Number of personal data breach notifications received</i> | 58 |
| <i>F. Personal data breach notification by sector</i> | 59 |
| <i>G. The nature and type of the personal data breach incident</i> | 61 |
| <i>H. The types of personal data affected</i> | 63 |
| <i>I. Monetary fines and other penalties</i> | 65 |
| <i>J. Measures taken to prevent or mitigate risk and impact evaluation</i> | 67 |
| <i>K. Use of PDBN data</i> | 68 |

| | |
|--|-----------|
| <i>Glossary of Terms</i> | 70 |
| ANNEX B. Survey questionnaire administered from June 2019 to February 2020 | 72 |
| <i>A. General questions and authority profile</i> | 72 |
| <i>B. Authority's funding and human resources</i> | 73 |
| <i>C. Personal data breach notification reporting law, jurisdiction and exemptions</i> | 76 |
| <i>D. Personal data breach annual reporting</i> | 79 |
| <i>E. Number of personal data breach notifications received</i> | 80 |
| <i>F. Personal data breach notification by sector</i> | 81 |
| <i>G. The nature and type of the personal data breach incident</i> | 83 |
| <i>H. The types of personal data affected</i> | 86 |
| <i>I. Monetary fines and other penalties</i> | 88 |
| <i>J. Measures taken to prevent or mitigate risk and impact evaluation</i> | 90 |
| <i>K. Use of PDBN data</i> | 91 |
| <i>Glossary of Terms</i> | 93 |
| Notes | 95 |

FIGURES

| | |
|---|----|
| Figure 1. Budgets of PEAs in 2018 and 2019 which are compared to that in 2017 among GDPR and non-GDPR countries (excluding the US) (n=26) (QB2) | 13 |
| Figure 2. Composition of authorities by types of funding (QB3) | 14 |
| Figure 3. Numbers of staff in PEAs in 2018 and 2019 from 2017 to 2019 that are compared to that in 2017 among GDPR and non-GDPR countries excluding the US (n=14) | 15 |
| Figure 4. Number of staff in the department/division/section that deals with PDBNs in 2017, 2018 and 2019 (in absolute numbers) | 16 |
| Figure 5. Number of countries that answered they have mandatory PDBN reporting to one or more authorities | 17 |
| Figure 6. Reported thresholds in US States (n=16, multiple answer is allowed) (QC3) | 20 |
| Figure 7. Timeframe with which PDBNs are required to report to the authority (QC4) | 21 |
| Figure 8. Whether the mandatory PDBN includes specific requirements for data subject notification (QC5) | 22 |
| Figure 9. Proportion of authorities that require mandatory PDBN reporting to the authority and have a central database that consolidates all DBNs reported (QC6) | 22 |
| Figure 10. Proportion of authorities with PDBNs statistics publicly available (QD1) | 23 |
| Figure 11. Publication of data/statistics on PDBNs at least once a year (QD1a) | 24 |
| Figure 12. Proportion of authorities that can provide to the OECD collected data of relevance to this survey (QD2) | 25 |
| Figure 13. Change in the number of PDBNs from 2017 to 2018 and from 2018 to 2019 in GDPR countries (QE2) | 26 |
| Figure 14. Distribution of percentage change in the number of PDBNs from 2017 to 2018 and from 2018 to 2019 in GDPR countries (QE2) | 27 |
| Figure 15. Annual number of data breaches and exposed records in the US from 2005 to 2009 | 28 |
| Figure 16. Proportion of authorities that recorded the total number of individuals that were affected in 2017 through 2019 (QE3) | 29 |
| Figure 17. Proportion of authorities that recorded PDBNs by sector in which breaches occur (QF1) | 29 |
| Figure 18. Industrial classifications used to report on PDBNs by sector (QF3) | 30 |
| Figure 19. Proportion of PDBNs by sector in six GDPR countries in 2019 (QF4) | 31 |
| Figure 20. Proportion of PDBNs by sector for three non-GDPR countries in 2019 (QF4) | 32 |
| Figure 21. Proportion of authorities that collect information on the nature and types of personal data breach incidents (QG1) | 33 |

| | |
|---|----|
| Figure 22. Proportion of authorities that can classify PDBNs into availability, integrity, and confidentiality breaches (QG2) | 33 |
| Figure 23. Proportion of authorities that answered they collect information on the types of personal data breached (QH1) | 35 |
| Figure 24. Proportion of authorities that answered they collect information on encryption of personal data breached (QH3) | 36 |
| Figure 25. Proportion of authorities that answered fines are administered for personal data breaches in their jurisdictions (QI1) | 37 |
| Figure 26. Proportion of authorities responsible for administering fines (QI3) | 37 |
| Figure 27. Proportion of authorities that are able to impose regulatory actions other than a fine in response to a PDBN or lack of breach notification (QI4) | 38 |
| Figure 28. Proportion of authorities that answered they verify the authenticity of reported PDBNs (QJ1) | 40 |
| Figure 29. Proportion of authorities that investigate what organisational and technical measures were in place the breached organisation prior to the data breach (QJ2) | 40 |
| Figure 30. Proportion of authorities that answered they investigate the economic and social impacts on the organisation that reported a personal data breach (QJ3) | 41 |
| Figure 31. Proportion of authorities that answered they use the PDBN data for budget planning for the next year and improving operation within the authority (QK1) | 42 |
| Figure 32. Proportion of authorities that use PDBN data for improving public relations to raise awareness of targeted sectors and entities and certain risks (QK2) | 43 |
| Figure 33. Proportion of authorities that use PDBN data for reinforcing collaboration with other authorities responsible for digital security, consumer policy, law enforcement, etc. (QK4) | 44 |
| Figure 34. Proportion of authorities that use PDBN data to evaluate the economic impacts of personal data breaches within their jurisdiction or their geographical scope (QK5) | 45 |

TABLES

| | |
|---|----|
| Table 1. Respondent countries | 11 |
| Table 2. Coverage of supervision on privacy protection practices by sector (QA5) | 11 |
| Table 3. Regulatory or oversight functions of respondent authorities in GDPR and non-GDPR countries other than the roles under a data protection or privacy law mandate and power (QA6) | 12 |
| Table 4. Regulatory or oversight functions of respondent authorities in US States other than the roles under a data protection or privacy law mandate and power (QA6) | 12 |
| Table 5. Number of countries that answered they have additional funding sources beyond 'Government funding' (by source) (QB3) | 14 |
| Table 6. Timing of the introduction of mandatory PDBN reporting to the authority (QC2) | 17 |
| Table 7. Thresholds to notify the authority in GDPR and non-GDPR countries (QC3) | 18 |
| Table 8. Reported thresholds by the number of the affected individuals to notify the authority (n=7) (QC3) | 20 |
| Table 9. Proportion of authorities that answered it is possible to classify personal data breaches by nature of causes (QG3) | 34 |
| Table 10. Proportion of authorities that answered it is possible to classify the PDBN data into specific sub-categories (QG8) | 35 |
| Table 11. Proportion of authorities that answered it is possible to classify the PDBN data that are collected into the following sub-categories (QH2) | 36 |
| Table 12. Proportion of authorities that answered they initiated audits/investigations in response to the following sources of information (QI5) | 39 |
| Table 13. Proportion of authorities that investigate various economic and social impacts on the organisation that reported a PDBN (QJ3) | 41 |
| Table 14. Proportion of authorities that use PDBN data for improving specific guidelines that data controllers are required to implement (QK3) | 43 |
| Table 15. Potential set of workable questions to improve comparability | 46 |

Executive summary

Overview

The “Promoting Comparability in Personal Data Breach Notification Reporting” project aims to improve the evidence base for security and privacy policy making through the comparable data collection by privacy enforcement authorities (PEAs). To this end, the OECD conducted an online survey to PEAs from June 2019 to February 2020. It sought to examine whether PEAs collect, or may be able to collect, a core set of administrative and technical data to improve comparability of personal data breach notification (PDBN) reporting and to assess potential statistical uses for those data.

By 14 February 2020, 32 OECD members and 3 non-members had responded to the questionnaire (20 European Union [EU] countries and 15 non-EU countries). The non-EU responses included answers from 23 US states and one US territory, which are collectively referred to as “24 US states”. Answers from EU and European Economic Area member countries were often similar, largely due to the impact of the General Data Protection Regulation (GDPR).

Since not all countries responded to each question, total responses do not always add up to 35. For the sake of readability, the findings below are often presented without attribution. However, in all cases, they are based on responses from the survey.

Major findings

- *Authority’s funding and resources*

Most countries have been increasing the financial resources of their PEAs. GDPR and non-GDPR countries generally tend towards 100% government-funded, while the US states generally reported mixed funding sources. Generally, reporting countries have more staff to respond to PDBNs.

- *PDBN reporting law, jurisdiction and exemptions*

In addition to GDPR countries, most non-GDPR countries and respondent US states have introduced a mandatory PDBN regulation. The remaining non-GDPR countries expect to introduce such a law within the next two years. However, countries frame and implement the regulation differently.

There is a general increase in the number of PDBNs that are reported to PEAs. This could indicate that PEAs are under operational pressure to process the increasing number of PDBNs. Thresholds to notify the authority about a data breach are generally risk-based but vary among jurisdictions and sectors. Around half of respondents with a mandatory PDBN also use a central database for internal monitoring, analysis and investigation.

- *Personal data breach annual reporting*

PDBN statistics are publicly available in more than 80% of GDPR countries, more than 50% of non-GDPR countries and more than 40% of US states. However, the type of information made available on data breaches varies.

- *Number of personal data breach notifications received*

There is a general increase in the number of PDBNs across countries.

- *Data breach notification by sector*

Eleven of 23 GDPR countries, 6 of 11 non-GDPR countries and 5 of 24 US states record PDBNs by sector. These numbers are slightly higher for authorities with mandatory PDBN. Most countries replied they used their own classifications, which reduces international comparability.

- *Nature and type of personal data breach incident*

Twenty of 23 GDPR countries, 9 of 11 non-GDPR countries and 12 of 24 US states collect information on the nature and types of personal data breach incidents. These numbers are higher when the analysis is restricted to authorities with mandatory PDBN reporting to the authority.

- *Types of personal data affected*

All but 3 of 23 GDPR countries (83%), 9 of 11 non-GDPR countries (82%) and 14 of 24 US states (54%) collect information on the types of personal data breached, at least for a subset of their PDBN data. Authorities with mandatory PDBN reporting to the authority were more likely to collect this information.

- *Monetary fines and other penalties*

All the GDPR countries, 6 of 11 non-GDPR countries and 15 of 24 US states administer fines for personal data breaches in their jurisdictions. Respondents in non-GDPR countries with a mandatory PDBN reporting to the authority are more likely to administer fines.

- *Measures taken to prevent or mitigate risk and evaluating PDBN impacts*

In 18 of 23 GDPR countries (78%), 8 of 11 non-GDPR countries (73%) and 20 of 24 US states (83%), authorities verify the measures in place in the breached organisations. A few authorities in GDPR and non-GDPR countries investigate the economic and social impacts of data breaches.

- *Use of PDBN data*

In 11 of 23 GDPR countries, 4 of 11 non-GDPR countries and 2 of 24 US states, authorities use the data for budget planning for the next year and improving operations. More than 50% of GDPR and non-GDPR countries and around 30% of the US states use PDBN data to improve guidelines for data controllers.

Conclusions

- *Internationally comparable data metrics*

Many authorities commonly collected data on the nature of causes (e.g. digital vs non-digital, malicious vs non-malicious, internal vs external), specific causes (e.g. mailing, hacking, theft), and types of data breached (e.g. personal credentials, financial, sensitive, encrypted). More than half of countries with mandatory PDBN reporting to the authority could provide PDBN data relevant to this survey to the OECD.

- *Types of questions suitable for internationally comparable data collections by PEAs.*

The survey identified questions for internationally comparable data collections by PEAs. These include areas such as sectoral application of mandatory PDBN; trigger and timeframe to notify the authority and data subjects; existence of a central database for data aggregation; industrial classification used on reported data breaches; sources of information to initiate investigations; measures taken by a breached firm; and use of collected data for enforcement collaboration. These questions can help build

comparability of future surveys on data breach, and regulatory actions and obligations. An annex suggests a structure for these questions in a revised questionnaire.

- *Possible challenges to improve international comparability*

Many authorities use their own industry classifications instead of the international standard (ISIC). Less than half use a central database for monitoring, analysis and investigation.

- *Monitoring the evolving environment*

Data metrics must evolve as malicious actors change their methods in response to new regulatory and other defences. Additionally, regulatory changes may diversify requirements and procedures for notifying data breaches. Therefore, monitoring the evolving context is also key to improving international comparability.

- *Next steps*

The OECD will continue to investigate these issues, focusing on consumers as data subjects. The aim is to examine consumer reactions to class action notices, data breach notifications and product recall notices. This work will be in collaboration with the Committee on Consumer Policy's Working Party on Consumer Product Safety and the Committee on Digital Economy Policy's Working Party on Data Governance and Privacy.

Introduction

The project on “Promoting Comparability in Personal Data Breach Notification Reporting” is part of a broader effort to improve the evidence base for security and privacy policy making. This work has been carried out since 2017 under the supervision of an international Expert Group, drawing from the Working Party on Security and Privacy in the Digital Economy (SPDE, now the Working Party on Data Governance and Privacy in the Digital Economy [DGP]) and the Working Party on Measurement and Analysis of the Digital Economy (MADE). Consequently, it brings a range of relevant expertise to this initiative.

The scope and objectives of this work were examined in DSTI/CDEP/SPDE(2017)1 and discussed with privacy enforcement authorities (PEAs) at a meeting of the International Conference of Data Protection and Privacy Commissioners (ICDPPC, now the Global Privacy Assembly) in September 2017.

A subset of administrative and technical data collected by PEAs on personal data breach notifications (PDBNs) and the potential statistical uses that might be made of that data were further examined in DSTI/CDEP/SPDE(2018)6 and discussed by the SPDE in May 2017. Delegates agreed that next steps should include a feasibility study on whether PEAs collect, or may be able to collect, the proposed set of data. To this end, the Secretariat developed an online questionnaire (DSTI/CDEP/SPDE(2018)13) that was circulated to PEAs with the support of the ICDPPC, the Asia Pacific Privacy Authorities (APPA) and the European Data Protection Board (EDPB). Key findings from the responses to the questionnaire were discussed at the joint OECD-ICDPPC expert consultation on 19 October 2018 and at the 44th meeting of SPDE. Following these meetings, the questionnaire was further revised to reflect comments received and circulated for a final round of comments in March 2019. The revised questionnaire (DSTI/CDEP/SPDE(2019)6) was circulated to PEAs in June 2019 with the support of the ICDPPC, the APPA and the EDPB.

This report presents key findings from the responses to the questionnaire. It was presented at the 21-22 April 2020 and the 7 April 2021 Virtual meetings of the Working Party on Data Governance and Privacy (DGP). It was subsequently circulated to the WPMADe delegates through written procedure from July 2020 to August 2020. The Committee on Digital Economy Policy (CDEP) approved and declassified the report by written procedure on 31 August 2021; the OECD Secretariat prepared it for publication.

Analysis of the responses

The questionnaire (Annex A), was developed by the OECD Secretariat. It aimed to examine whether PEAs collect, or may be able to collect, a core set of administrative and technical data to improve comparability of PDBN reporting and to assess potential statistical uses for those data [DSTI/CDEP/SPDE(2018)13]. It included 11 sections:

- A. General questions and authority profile
- B. Authority's funding and resources
- C. Personal data breach notification reporting law, jurisdiction and exemptions
- D. Personal data breach annual reporting
- E. Number of personal data breach notifications received
- F. Personal data breach notification by sector
- G. The nature and type of the personal data breach incident
- H. The types of personal data affected
- I. Monetary fines and other penalties
- J. Measures taken to prevent or mitigate risk and impact evaluation
- K. Use of PDBN data

The questionnaire was circulated to PEAs from June 2019 to February 2020 through the ICDPPC (renamed Global Privacy Assembly in 2019), the APPA and the EDPB. The next sections of the document discuss the main findings.

A. Authority profiles

Respondent countries

By 14 February 2020, 35 countries had responded to the questionnaire, consisting of 20 European Union (EU) countries and 15 non-EU countries. Responses were sought from each state in the United States because data breach notification is mostly regulated at the state level.¹ Responses were received from 23 US states and one US territory, which are collectively referred to as "24 US states". A total of 32 OECD member countries and 3 non-members responded to the questionnaire (Table 1).

Table 1. Respondent countries

| | Countries bound by the GDPR (“GDPR countries”) (23) | Non-GDPR countries (12) |
|----------------------------|---|---|
| EU countries (20) | Austria, Czech Republic, Estonia, Finland, France, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden (20) | None |
| Non-EU countries (15) | Liechtenstein, Norway, United Kingdom* (3) | Australia, Canada, Chile, Colombia, Korea, Japan, Mexico, New Zealand, Turkey, Singapore, Switzerland, United States (23 states and 1 territory) (12) |
| OECD member countries (32) | Austria, Czech Republic, Estonia, Finland, France, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, United Kingdom (21) | Australia, Canada, Chile, Colombia, Korea, Japan, Mexico, New Zealand, Turkey, Switzerland, United States (23 states and 1 territory) (11) |
| Non-OECD countries (3) | Liechtenstein, Malta (2) | Singapore (1) |

* The United Kingdom left the European Union in January 2020. Domestic legislation maintains the same level of privacy protection as the GDPR.

The commonality in PDBN regulations depends largely on geography. The answers from EU and European Economic Area member countries were often similar, largely due to the impact of the General Data Protection Regulation 2016/679 (GDPR).² In the United States, starting with California in 2002, all 50 states and several territories have now enacted data breach notification laws.³ Therefore, for this report, the following categorisation was adopted: i) “GDPR countries” denote the 23 countries bound by the GDPR (plus the United Kingdom); ii) “non-GDPR countries” denote the remaining 11 countries (excluding the United States); and iii) “US states” denote the 23 US states and 1 US territory that responded to the survey.

Oversight and law enforcement

Respondent authorities were asked if they are involved in enforcing regulations on PDBN in QA4 of the questionnaire. Among all respondents, 31 authorities answered they are, while one GDPR country answered, “Do not know”. Three non-GDPR countries answered “No”, and also stated (in QC1) that they do not have a mandatory PDBN reporting obligation. This suggests those non-GDPR countries may have assumed that “enforcing regulation” meant existence of mandatory regulation.

The authorities were also asked if they oversee privacy protection practices by the public, private and non-profit sectors in QA5. The private sector is covered in almost all GDPR, non-GDPR and US states, while the public and non-profit sectors are covered by a smaller number of countries (Table 2).

Table 2. Coverage of supervision on privacy protection practices by sector (QA5)

| | Public sector | Private sector | Non-profit sector (NPOs, charities, etc.) |
|---------------------------|---------------|----------------|---|
| GDPR countries (n=23) | 100% (23) | 100% (23) | 96% (22) |
| Non-GDPR countries (n=11) | 91% (10) | 91% (10) | 82% (9) |
| US states (n=24) | 79% (19) | 100% (24) | 83% (20) |

Note: The numbers in parentheses represent the number of countries that answered they cover each sector overseeing privacy protection practices. NPO=non-profit organisation.

Additional functions under national laws

Respondent authorities were asked if they have regulatory or oversight functions other than data protection or privacy law enforcement (in QA6). Twelve of the 23 GDPR countries and 7 of the 11 non-GDPR countries answered they do. Many authorities have a role in enforcing and overseeing their national Freedom of Information laws (six GDPR countries and four non-GDPR countries). Some have also oversight roles for privacy protection in specific sectors (such as telecommunications). Furthermore, some oversee potential breaches of unsolicited communication regulation (e.g. unsolicited telemarketing, commercial emails and short message services). In addition, a few authorities answered they have other broad enforcement responsibilities including for the protection of children on line (Table 3). Notably, 16 US states answered they have a wide range of other regulatory or oversight functions in QA6 (Table 4).

The open-ended question style of QA6 led to responses varying in terms of detail and organisational scope from the US states. For example, some answered for the whole Office of Attorney General or Department of Justice, while others focused only on the specific unit within. In fact, the literature notes that all states have consumer protection and freedom of information laws in the United States.⁴

Table 3. Regulatory or oversight functions of respondent authorities in GDPR and non-GDPR countries other than the roles under a data protection or privacy law mandate and power (QA6)

| | GDPR countries (n=12) | non-GDPR countries (n=7) |
|--|--------------------------|-----------------------------|
| Freedom of Information | 6 | 4 |
| Privacy protection in the telecommunication sector | 4 | 0 |
| Data protection in other sectors | 3 | 1 |
| Unsolicited communication regulation | 1 | 2 |
| Others | 3 | 1 |

Table 4. Regulatory or oversight functions of respondent authorities in US states other than the roles under a data protection or privacy law mandate and power (QA6)

| | Number of authorities (n=16) |
|--|---------------------------------|
| Freedom of Information | 4 |
| Consumer fraud and deceptive trades | 4 |
| Oversight of tobacco and alcohol sectors | 4 |
| All criminal prosecution | 3 |
| Consumer policy | 3 |
| Identity theft | 2 |
| Other | 8 |

B. Authority's funding and resources

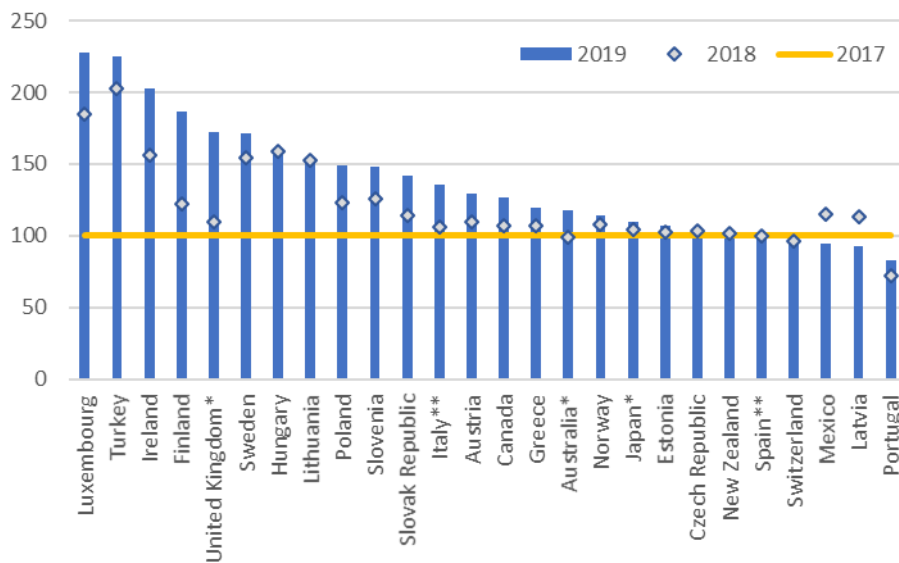
Financial resources

The questionnaire gathered detailed information on financial and human resources of respondent authorities. Twenty-six of the 34 countries (excluding the United States) and five US states provided budget information on successive three reference periods: 2017 through 2019 (QB2). The results demonstrate that most countries (22 of 26) have been increasing the financial resources of their PEAs (Figure 1). This trend appears consistent with results that indicate many authorities consider the number of PDBNs when allocating budgets and resources (QK1) and with the data collected in Section E, indicating an increasing

trend in the number of PDBNs. QB2, which asked about the total budget of the respondent authority or the budget dedicated to PEA-type work, may not have been clear enough. Some authorities answered they do not know the total budgets of the authority in 2019, 2018 and 2017. They also commented they have roles other than PEA responsibility and no separate budget figure for the PEA work. To clarify and accommodate different circumstances, maybe there should be two separate questions asking the total budget and the budget dedicated to PEA-type work, respectively.

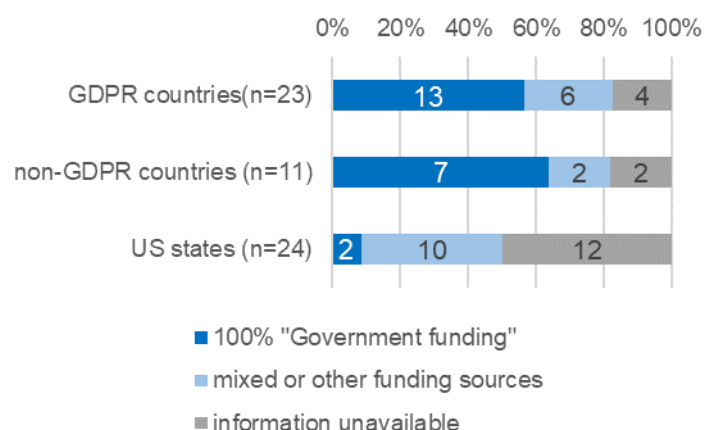
Figure 1. Budgets of PEAs among GDPR and non-GDPR countries (excluding the United States) (n=26) (QB2)

Budgets in 2017 are normalised to 100. Budgets in 2018 and 2019 are compared against this normalised value.⁵



Note: * Refers to countries reporting according to fiscal years. ** Refers to countries providing values between 2016 and 2018.

The questionnaire also collected information on the funding sources of the respondent authority and its composition (QB3). Most respondents provided this information (19 of 23 GDPR countries, 9 of 11 non-GDPR countries and 12 US states). The GDPR and non-GDPR countries generally tend towards 100% government-funded (13 of 19 GDPR countries and 7 of 9 non-GDPR countries, respectively, chose “Government funding” and put 100% as the proportion), while the US states generally reported mixed funding sources (Figure 2).

Figure 2. Composition of authorities by types of funding (QB3)

Note: The respondent countries that chose only "Government funding" are represented as "100% 'Government funding'". Those that chose "Government funding" plus more than one other alternative in QB3 are represented as "mixed funding sources".

Mixed funding includes a variety of sources (Table 5). Six GDPR countries and two non-GDPR countries answered they have "Chargeable Services", "Registration or licensing fees", "Fines and penalties" and "other" as funding sources. Ten US states answered they are funded by budget allocation plus other funding sources. Eight US states answered they rely on "Fines and penalties", four on "Registration or licensing fees", followed by three on "Other" and one on "Chargeable services" (Table 5). Other funding sources such as registration fees and fines are government funds, too, when they are created by laws. Therefore, "Budget allocation" is more relevant a term than "Government funding".

Although only five authorities reported on the composition of their mixed funding sources, most (four of five) answered they are predominately funded by "Government funding" (87-97%). The United Kingdom is the only country in the survey that answered it is financed almost entirely by "Registration or licensing fees" (97%).

Table 5. Number of countries that answered they have additional funding sources beyond "Government funding" (by source) (QB3)

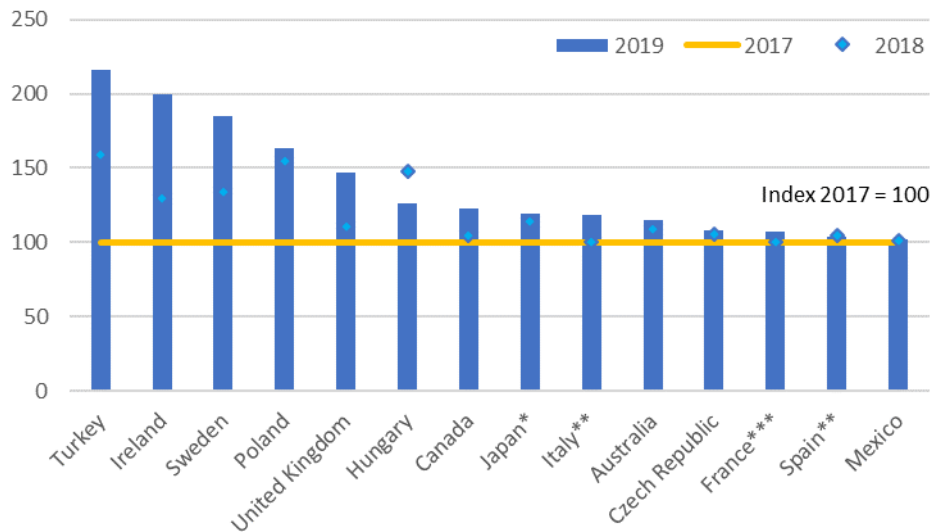
| | Chargeable services | Registration or licensing fees | Fines and penalties | Other |
|------------------|---------------------|--------------------------------|---------------------|-------|
| GDPR (n=6) | 3 | 2 | 1 | 1 |
| Non-GDPR (n=2) | 2 | 1 | 0 | 1 |
| US states (n=10) | 1 | 4 | 8 | 3 |

Note: Among GDPR countries, in addition to "Government funding", Estonia, Finland and Latvia are funded by chargeable services, Latvia and the United Kingdom are funded by registration or licensing fees, Portugal is funded by fines and penalties, and Italy is funded by administrative fee that was answered in "Other". Among non-GDPR countries, Australia is mostly resourced through "Government funding" and partially funded by "Chargeable services", New Zealand is funded by "Government funding", "Chargeable services", "Registration or licensing fees", and interest earned that was answered in "Other". Among the US states, in addition to budget allocation, Indiana is funded by "Chargeable services"; Delaware, Indiana, Iowa and South Carolina are funded by "Registration or licensing fees"; Arkansas, Delaware, Indiana, Iowa, Maine, Nevada, South Carolina and West Virginia are funded by "Fines and penalties"; and New Jersey (Agency revenue funds), South Carolina and Guam (Consumer Protection Fund) are funded by "Other" sources.

Human resources

Respondents were asked to specify the number of staff employed at their PEAs, as well as full-time or equivalent staff employed in the department, division or section that deals with PDBNs. All but one of the 23 GDPR countries, 9 of 11 non-GDPR countries and 8 of 24 US states provided the number of overall staff in PEAs in QB5. Among them, 19 GDPR countries, 6 non-GDPR countries and 7 US states provided the numbers for the years 2017 to 2019. Figure 3 represents changes in the number of staff in PEAs from 2017 to 2018 and 2019 and sheds light on recent changes, when pressure on PEAs was likely increasing due to regulatory developments. Numbers of staff in 2017 are normalised to 100. Numbers of staff in 2018 and 2019 are compared against this normalised value. To avoid overrepresentation of changes from small numbers, data fewer than 50 were eliminated from the calculation, where 9 of 19 GDPR countries and 5 of 6 non-GDPR countries have larger numbers than 50. All authorities with more than 50 staff members show an increasing trend in staff numbers.

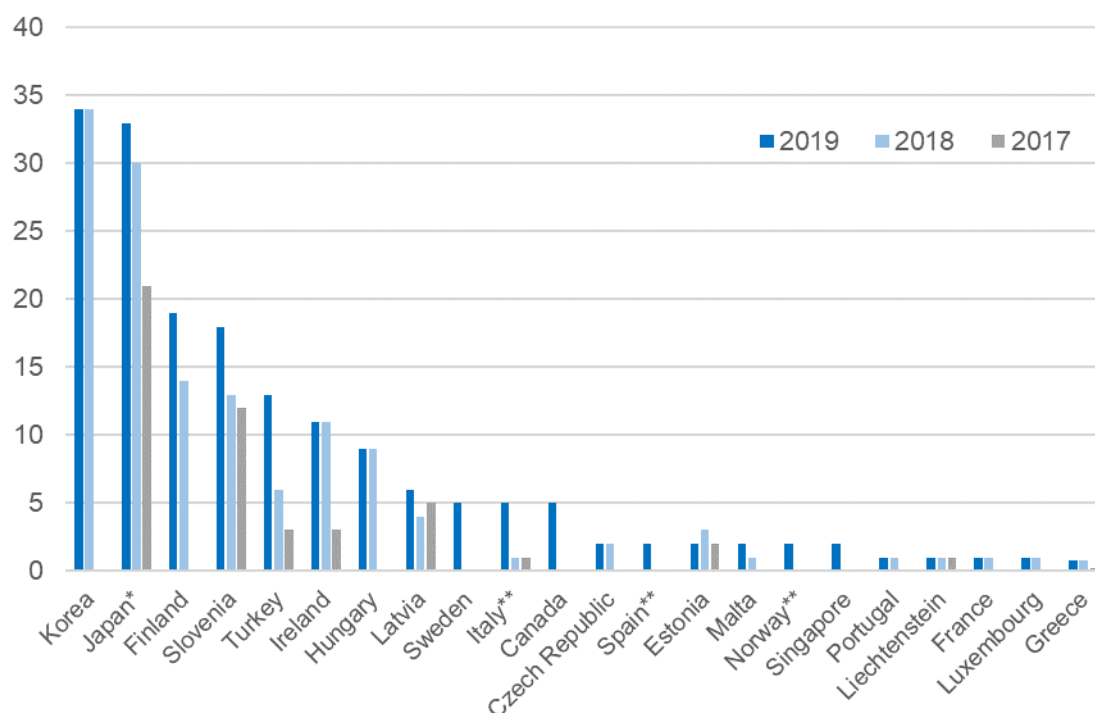
Figure 3. Numbers of staff in PEAs among GDPR and non-GDPR countries excluding the United States (n=14)



Note: * Refers to countries reporting according to fiscal years. ** Refers to countries providing values between 2016 and 2018. *** Refers to countries providing values only in 2018 and 2019. Therefore, the 2018 figures are normalised to 100.

Further, 17 of 23 GDPR countries, 5 of 11 non-GDPR countries and 13 US states provided the number of staff employed in the department, division or section that deals with PDBN in QB5. Although some provided the number for only one or two years of the most recent reference periods, Figure 4 indicates a general increase in the reporting countries of the number of staff employed to respond to PDBNs. In particular, three countries reported having newly hired staff to deal with PDBNs during the most recent reference periods. A number of US states mostly deal with personal data breaches on a case-by-case basis by staff assigned to general enforcement. Only a few US states indicated they employ staff dedicated to PDBNs, although US states have had breach notification laws for several years, starting with California in 2002.

Figure 4. Number of staff in the department/division/section that deals with PDBNs



Note: * Refers to countries reporting according to fiscal years. ** Refers to countries providing values between 2016 and 2018.

C. PDBN reporting law, jurisdiction and exemptions

1. PDBN reporting to the authority

There is a general trend towards mandatory PDBN reporting

Respondents were asked if there is any mandatory requirement for data controllers to report personal data breaches to one or more enforcement authorities in their jurisdictions (in QC1). If they did not have such a requirement, countries were asked if any PDBNs would become mandatory in the next two years (in QC1a). As the results of the pilot survey in 2018 indicated, there is a general trend towards mandatory PDBN reporting. Figure 5 shows the number of countries that answered they have mandatory PDBN reporting to one or more authorities. All GDPR countries, 6 of the non-GDPR countries and 16 US states answered they have introduced a mandatory PDBN reporting to one or more authorities. The remaining five non-GDPR countries responded they expected to introduce such a law within the next two years. The years of introduction of mandatory PDBN reporting also show this is a recent trend outside the United States. It followed the early introduction of PDBN by some states over ten years ago, originating in California in 2002⁶ (Table 6). The analysis of responses to Section C is restricted to countries that answered they have introduced a mandatory PDBN reporting in QC1, as QC1 is a filter question for the rest of the questions in Section C.

While many authorities are introducing mandatory PDBN reporting, there are significant differences across countries in the way regulation is framed and implemented. Simple comparison is therefore not possible and may potentially lead to misinterpretation or a misunderstanding of the situation behind the data.

Figure 5. Number of countries that answered they have mandatory PDBN reporting to one or more authorities

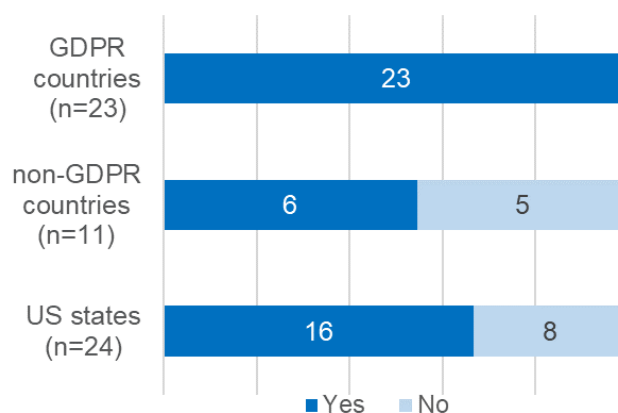


Table 6. Timing of the introduction of mandatory PDBN reporting to the authority (QC2)

| | Year of implementation |
|----------------|--|
| GDPR countries | 2018 for public and private sectors 2014 for telecom sector |
| Canada | 2018 for private sector, 2014 for public sector |
| Australia | 2018 for public and private sectors |
| Mexico | 2017 for public sector |
| Turkey | 2016 for public and private sectors |
| US states | 2019 (1), 2018 (1), 2012 to 2014 (4), 2005 to 2009 (7) |

Mandatory PDBN reporting to the authority applies differently to the public and private sectors.

Any system of notification may be universal, such as one applied through a country's national data protection law. It may be regionally based and therefore applied through legal requirements at state or provincial level. Finally, it may be sector-based through laws and/or codes or practices that are focused on the health or the financial services sector. In some cases, notification requirements apply differently between public and private sector organisations (Table 7).

In the European Union, the GDPR covers public and private sectors, and the ePrivacy Directive additionally applies to the EU telecom sector. In Mexico, mandatory PDBN reporting applies only to "Obligated Parties", which includes the public sector. In Australia, mandatory PDBN reporting applies to both public and private sectors. However, Australia exempts private sector organisations with an annual turnover of less than AUD3 million except for private sector health service providers, credit reporting bodies, credit providers and entities that trade in personal information and tax file number recipients. In Canada, government institutions are required to report material privacy breaches to the Office of the Privacy Commissioner of Canada (OPC) and the Treasury Board Secretariat. Likewise, private sector organisations in Canada are required to report any breaches that represent a risk of significant harm to OPC.⁷ In Korea, mandatory PDBN reporting applies to both public and private sectors when personal information of over 1 000 data subjects is divulged. Among the 16 US states that answered they have a mandatory PDBN reporting to

the authority, 14 said it applies to all sectors. Some US states noted exceptions and special requirements for certain sectors such as health and banking, which need to comply with the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act, respectively.

Table 7. Thresholds to notify the authority in GDPR and non-GDPR countries (QC3)

| | Triggers |
|--|---|
| GDPR countries | Any breach that poses a risk of harm to or adverse effect on the data subject for public and private sectors. Unauthorised access, deletion and alteration, regardless of risk of harm to or adverse effect on the data subject for the telecom sector. |
| Mexico | Any breach that poses a risk of harm to or adverse effect on the data subject for the public sector. |
| Turkey | Unauthorised access, deletion, alteration and acquisition, regardless of risk of harm to or adverse effect on the data subject for public and private sectors. |
| Canada | “Other”: Government institutions are required to report material privacy breaches to the Office of the Privacy Commissioner of Canada and the Treasury Board Secretariat. A breach is deemed “material” if the breach: i) involves sensitive personal information; and ii) could reasonably be expected to cause serious injury or harm to the individual and/or involves a large number of affected individuals. Private organisations are required to notify the authority when it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual. As well, notification to other organisations or government institutions will be required if the notifying organisation believes the other organisation or government institution or part concerned may be able to reduce the risk of harm that could result from it or mitigate that harm. |
| Australia | “Other”: Regulated entities are required to notify “eligible data breaches”, which are defined as: unauthorised access to, unauthorised disclosure of or loss of personal information that is likely to result in serious harm to any affected individual, where the entity has not been able to prevent the likely risk of serious harm with remedial action. ⁸ |
| Washington State (as an example of the US state) | “Other” There is a requirement to provide notice to individuals whose personal information was, or is reasonably believed to have been, acquired by an unauthorised person. Notice is not required if the breach is not reasonably likely to subject consumers to a risk of harm. If required to notify more than 500 Washington residents as a result of a single breach, the entity is also required to notify the attorney general. ⁹ |

Thresholds to notify the authority are generally risk-based but vary among jurisdictions and sectors

The questionnaire collected information on the thresholds of PDBN notification to the authority in QC3. Almost all GDPR countries answered that the PDBN is triggered by “any breach that poses a risk of harm to or adverse effect on the data subject” (22 of 23), reflecting requirements in Articles 4(12)¹⁰ and Article 33(1)¹¹ of the GDPR. Some countries added that it is also triggered by “unauthorised access, deletion and alteration, regardless of risk of harm to or adverse effect on the data subject” (4 of 22), reflecting requirements in Articles 2(h)¹² and 4(3)¹³ of the ePrivacy Directive.

Turkey indicated that PDBN is triggered by “unauthorised access, deletion, alteration and acquisition, regardless of risk of harm to or adverse effect on the data subject”. The Turkish Personal Data Protection Law requires data controllers to notify the authority if the personal data processed are obtained by others by unlawful means, irrespective of a risk of harm to data subjects. It prescribes that the authority publicly announce such breach on its official website or any other way, depending on the risk of harm to data subjects.¹⁴

Mexico reported that its PDBN is triggered by “any breach that poses a risk of harm to or adverse effect on the data subject”. The PDBN can also be triggered by “other”, emphasising that theft or loss of personal

information is also recognised as a data breach.¹⁵ This reflects the General Law on Protection of Personal Data Held by Obligated Parties (2017), which requires notification of breaches that significantly affect economic or moral rights.¹⁶

In Canada and Australia (which chose “other” as their response), thresholds are generally based on a risk-based approach. They depend on the likelihood that access, disclosure and loss result in serious harm to any of the individuals to whom the information relates (Table 7).¹⁷ Whether a data breach is likely to result in serious harm requires an objective assessment. For the Notifiable Data Breach (NDB) scheme in Australia, the phrase “likely to occur” means the risk of serious harm to an individual is more probable than not (rather than possible). “Serious harm” is not defined in the Privacy Act 1988. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial or reputational harm. The NDB scheme includes a non-exhaustive list of “relevant matters” that may assist entities to assess the likelihood of serious harm. These are set out in the Privacy Act.

In Korea, the Personal Information Protection Act requires the data controller to notify data subjects when the data controller is aware that their personal information is divulged, irrespective of risk of harm to the data subjects or of the number of the affected data subjects. The act also requires the data controller to notify the Personal Information Protection Commission and the Korea Internet & Security Agency and to post the relevant matters about the breach on their websites for more than seven days, when personal information of over 1 000 data subjects is divulged.¹⁸

The response to QC3 of the 16 US states with a mandatory PDBN reporting varied significantly (Figure 6). The literature notes that many US states do not have a threshold that depends on the degree of harm to data subjects. Others with such a harm threshold focus typically on financial harm such as fraud and identity theft.¹⁹ PDBN regulations in the 16 US states generally require notification to the State Attorney General and/or other third parties such as the State Office of Consumer Protection. Often, this requirement depends on the number of individuals affected by the breach. For example, in Washington State, consumers have to be notified of any breach “reasonably likely to subject consumers to a risk of harm” (Table 7). Meanwhile, the Attorney General has to be notified of breaches affecting more than 500 individuals. However, in other cases, notification is required, irrespective of the number of affected individuals (Table 8). Therefore, the choices listed in the questionnaire were poorly adapted to the US context. In addition, although all the US states have a mandatory PDBN reporting to affected individuals, only 15 of 24 responded they have it in QC5 (see also below). This indicates room for improvement in the questionnaire. For instance, the questionnaire should be designed to ask separate questions about notification to affected individuals and questions about notification to the authority.

Figure 6. Reported thresholds in US states (n=16, multiple answer is allowed) (QC3)

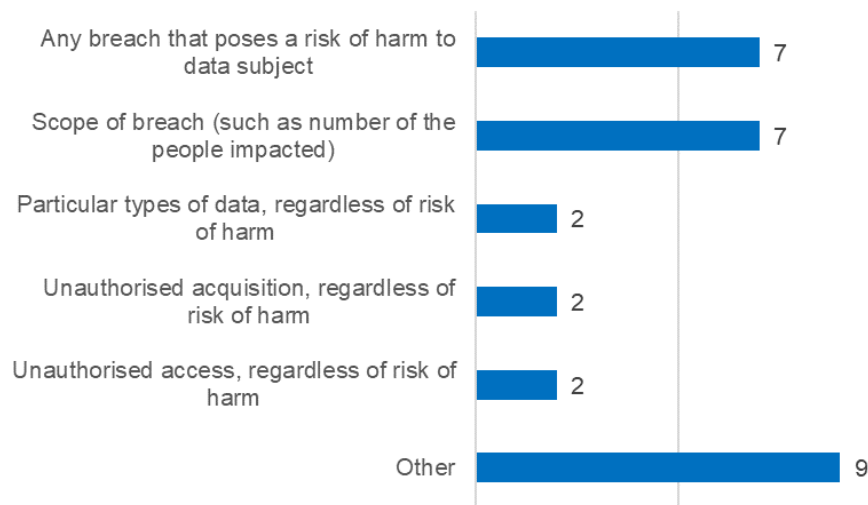


Table 8. Reported thresholds by number of affected individuals to notify the authority (n=7) (QC3)

| Number of affected individuals | States |
|--------------------------------|------------------------------------|
| 1 000 | Arkansas, Missouri, South Carolina |
| 500 | Delaware, Iowa, Washington, |
| 250 | Oregon |

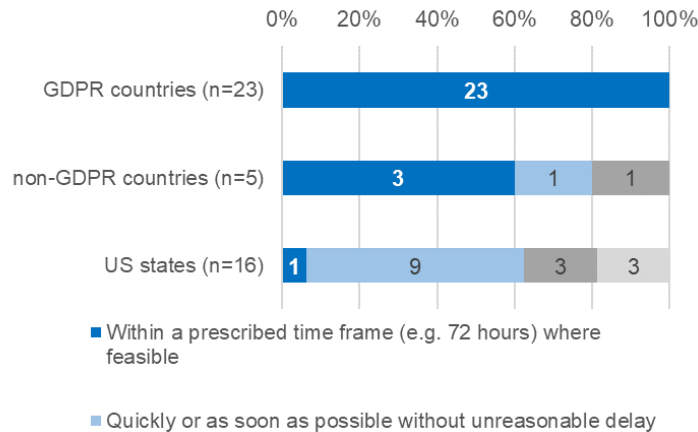
Prescribed timeframes within which authorities must be notified

The survey also collected information about the timeframe within which organisations are required to report data breaches to the relevant authority (QC4). All GDPR countries indicated that notification is required within 72 hours (Figure 7). This reflects conditions set by Article 33(1) of the GDPR. Some countries additionally cited requirements of the shorter timeframes of the ePrivacy Directive. Four of the six non-GDPR countries with mandatory PDBN also responded that notification must occur within a prescribed timeframe where feasible.

Canada differentiated between prescribed timeframes for the public sector and the private sector in its answer. For the private sector, the law requires notification to the authority as soon as feasible after an organisation has discovered a personal data breach. For the public sector, under the Directive on Privacy Practices, government institutions are responsible for establishing plans and procedures, including timing, for notifying material privacy breaches to the authority. However, the timeframe of this notification is not specified.

While 9 of 16 US states said that notification must be made “quickly or as soon as possible without unreasonable delay”, many also mentioned a prescribed timeframe. For instance, the State of Iowa requires notification to the Director of Consumer Protection within five days of notifying affected consumers. These consumers, in turn, must be notified in “the most expeditious manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement”.

Figure 7. Timeframe with which PDBNs are required to report to the authority (QC4)



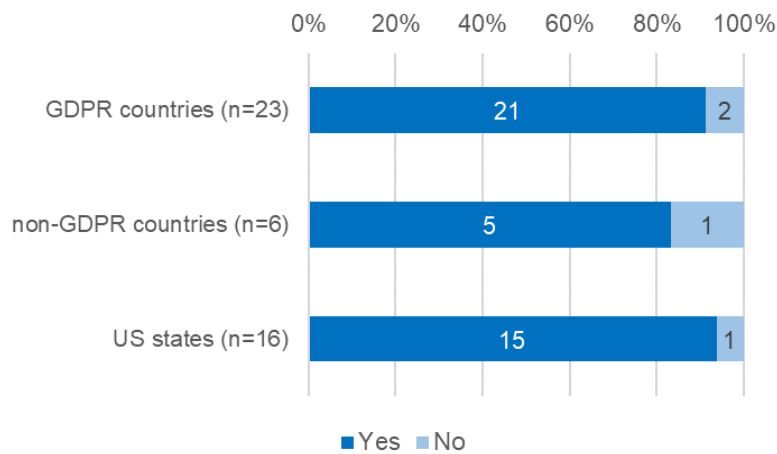
2. PDBN reporting to the data subjects

Question QC5 aimed to distinguish whether mandatory PDBN reporting also includes data subject notification requirement and whether these differ from requirements to notify the authority. For 21 GDPR countries, mandatory PDBN reporting also includes data subject notification breaches that might adversely affect them (Figure 8). Of these countries, 17 further answered that the requirements to notify data subjects are somewhat different from those to notify the authority. Many referred to Article 34(1)²⁰ of the GDPR and some also referred to Article 2(1) of EU Regulation 611/2013.²¹

Five of the six non-GDPR countries with mandatory PDBN reporting also answered that it includes specific requirements for data subject notification. Three of the five countries answered that requirements for PDBN reporting to the authority are the same as those to data subjects. Among the remaining two non-GDPR countries, in Turkey, the thresholds to notify the authority and data subjects are the same, but timeframes to notify are different. Data controllers are required to notify the authority without any delay and not later than 72 hours from the date following identification of persons affected by a data breach. Meanwhile, data subjects affected by the data breach should be notified as soon as possible. In Canada, for the private sector, there is no difference in requirements to notify data subjects and the authority. For the public sector, on the other hand, notification of data subjects and the authority is handled differently. Treasury Board Secretariat guidelines for privacy breaches strongly recommend that government institutions notify all individuals whose personal information has been, or may have been, compromised. At the same time, the guidelines indicate that institutions must establish a process for the mandatory reporting of material privacy breaches to the authority.

Fifteen of 16 US states with a mandatory PDBN reporting to the authority answered that the mandatory PDBN reporting to the authority includes specific measures to notify data subjects. Within these states, most (11 of 16) further answered that requirements to notify the data subject are not different from those to notify the authority. The remaining four states mentioned that notification to the authority depends on the number of affected individuals. They also referred to a difference in timeframe to notify. For instance, the notification to authority must occur when the breach is disclosed to affected individuals or within 45 days after the breached entity determines there is no reasonable likelihood of harm to the affected individuals, whichever occurs first.

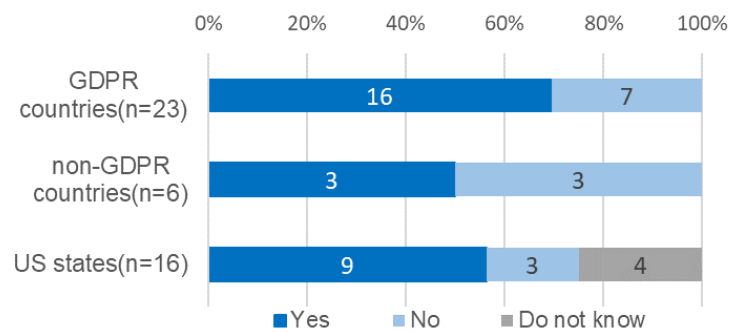
Figure 8. Whether the mandatory PDBN includes specific requirements for data subject notification (QC5)



3. Central database

Question QC6 covers the availability of a central database that consolidates all PDBNs reported in countries for activities such as internal monitoring, analysis and investigation. Around half of respondents that reported having a mandatory PDBN also reported the existence of such a central database. Sixteen of 23 GDPR countries, 3 of 6 non-GDPR countries and 9 of 16 US states with mandatory PDBN also answered they have a central database. This part of the questionnaire was not well suited to the United States, however, because a number of the states considered that “a central database” referred to a federal database.

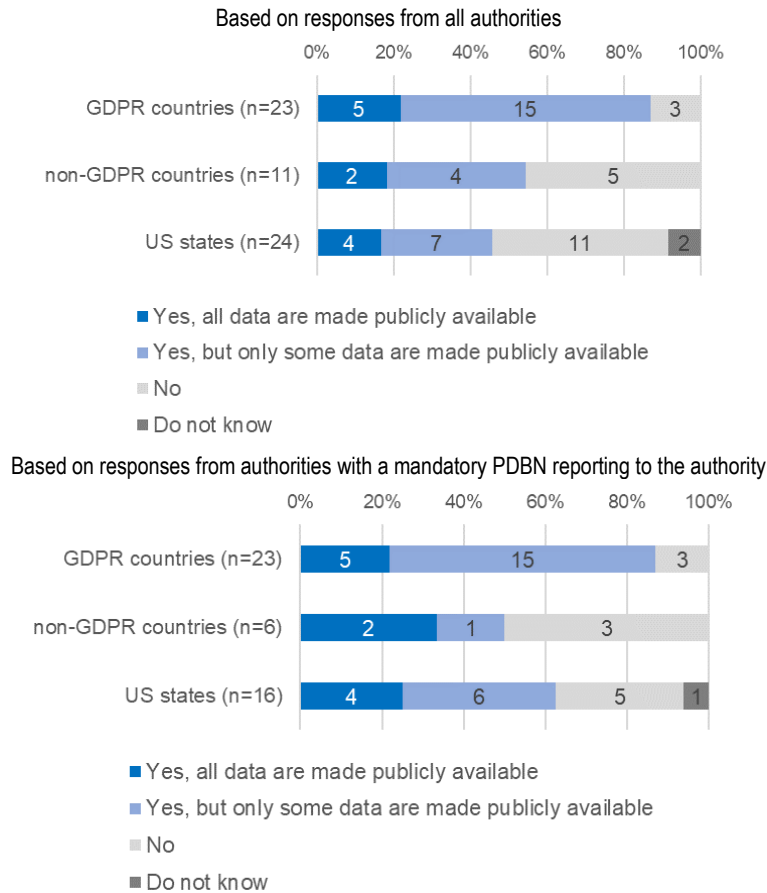
Figure 9. Proportion of authorities that require mandatory PDBN reporting to the authority with a central database that consolidates all DBNs reported (QC6)



D. Personal data breach annual reporting

More than 80% of GDPR countries, more than 50% of non-GDPR countries and more than 40% of US states answered that at least part of the PDBN statistics are publicly available (Figure 10). The same analysis on countries with mandatory PDBN reveals a slightly lower proportion of non-GDPR countries and a greater proportion of US states with PDBN statistics at least partly publicly available (50% of non-GDPR countries and 63% of US states).

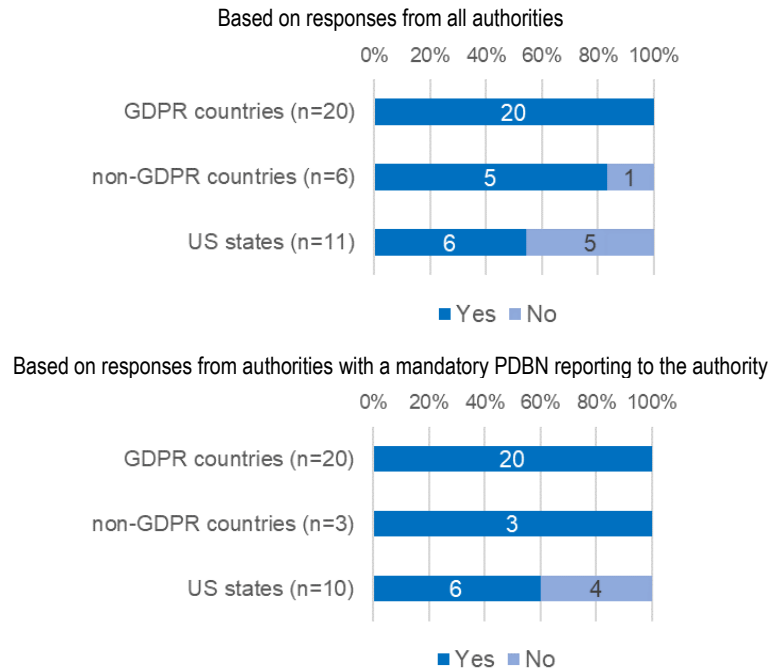
Figure 10. Proportion of authorities with PDBNs statistics publicly available (QD1)



All GDPR countries that said they made their PDBN statistics at least partially publicly available (in QD1) answered they published their data/statistics on PDBNs at least once a year (QD1a). Five of 6 non-GDPR countries and 6 of 11 US states answered in the same way (Figure 11).

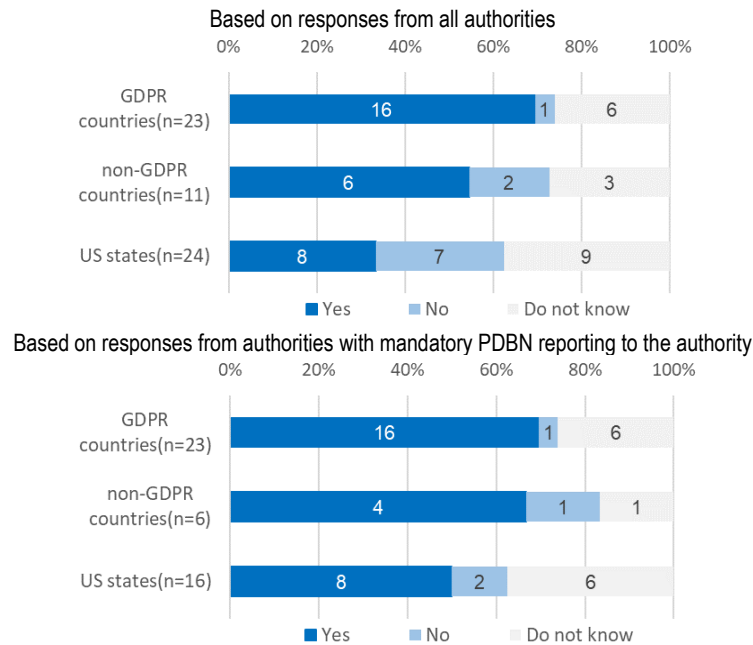
However, the type of information made available on data breaches varies. Some contains only breached data controllers' names, dates of breaches and notifications, and the number of affected individuals. Others contain types of information breached, date of discovery of breaches, notice letters, amount of compensation paid to affected individuals and so on.

Figure 11. Publication of data/statistics on PDBNs at least once a year (QD1a)



Sixteen of 23 GDPR countries, 6 of 11 non-GDPR countries and 8 of 24 US states answered they can provide available data relevant for this project to the OECD (QD2). The proportion increases for authorities with a mandatory PDBN reporting. Nearly 70% of GDPR countries (16 of 23), 67% of non-GDPR countries (4 of 6) and nearly 50% of US states (8 of 16) answered they can provide the collected PDBN data relevant to this survey to the OECD (Figure 12).

Figure 12. Proportion of authorities that can provide collected data relevant to this survey to the OECD (QD2)



E. Number of personal data breach notifications received

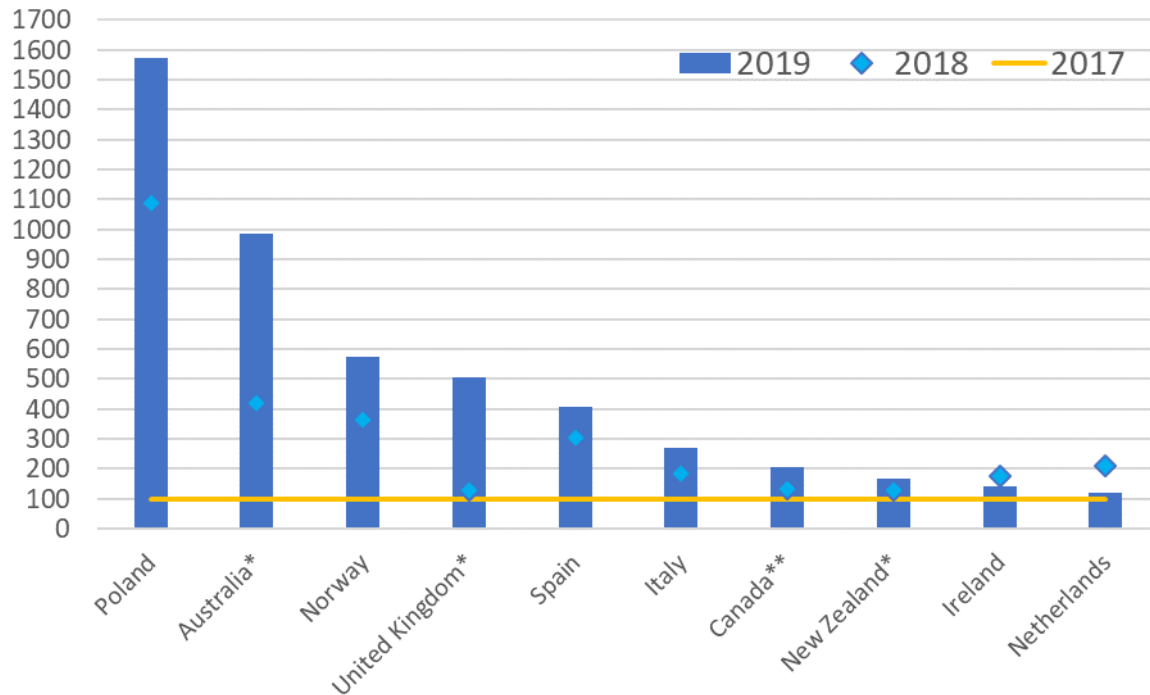
Question QE2a referred to the number of PDBNs under voluntary or mandatory arrangements that respondent authorities received in 2019, 2018 and 2017 or during other recent reference periods. Twenty-three GDPR countries, 6 non-GDPR countries and 14 US states provided their data for at least one reference period.

As in the last round of the survey in 2018, there is a general increase in the number of PDBNs across countries. In the analysis below, numbers are represented in terms of percentage change to uncover an eventual effect of the introduction of mandatory PDBN regulation, particularly in GDPR countries. This visualisation can also provide useful information for authorities on possible operational pressures. The data, however, need to be PDBN across countries, which does not lend itself to simple comparison. Indeed, the number of PDBNs ranges from the order of 1 to the order of 10 000.

According to the full set of data (for 2017, 2018 and 2019) provided by seven GDPR countries and three non-GDPR countries, the number of PDBNs has continuously increased (Figure 13). Data from three GDPR countries and one non-GDPR country are not used here to avoid overrepresentation of changes from small numbers. In ten countries, the normalised numbers of PDBNs in 2018 and 2019 are above 100.

Figure 13. Change in the number of PDBNs from 2017 to 2018 and from 2018 to 2019 in GDPR countries (QE2)

Numbers of PDBNs in 2017 are normalised to 100. Numbers of PDBNs in 2018 and 2019 are compared against this normalised value. To avoid overrepresentation of changes from small numbers, data fewer than 50 were eliminated from the calculation.

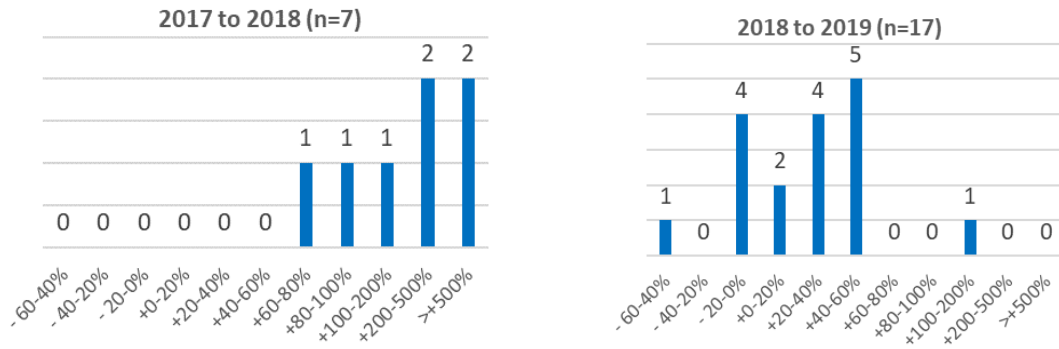


Note: * Refers to countries reporting according to fiscal year; ** Refers to countries that separately provided figures for public and private sectors, which are combined in the figure.

Figure 14 shows the distribution of percentage changes in the number of PDBNs from 2017 to 2018 and from 2018 to 2019 in GDPR countries. The numbers in seven countries from 2017 to 2018 and in those from 2018 to 2019 are larger than 50, the cut-off value. The changes show significant increases in PDBNs, probably due to the introduction of the GDPR and mandatory PDBN. In addition, from 2017 to 2018, three countries recorded their first PDBNs and another three countries experienced more than a tenfold increase. As some countries indicated data collection period in 2018 was May to December, the increase from 2018 to 2017 may be underrepresented.

Such significant increases may exert pressure on PEAs. These data confirm the results of a survey by the European Data Protection Board in May 2019 that show an increasing number of queries and complaints.²² The change from 2018 to 2019 also indicates a general increase in PDBNs. However, in countries with different reference periods in 2019 (between six to ten months), the change from 2018 to 2019 should be interpreted with caution.

Figure 14. Distribution of percentage change in the number of PDBNs in GDPR countries (QE2)

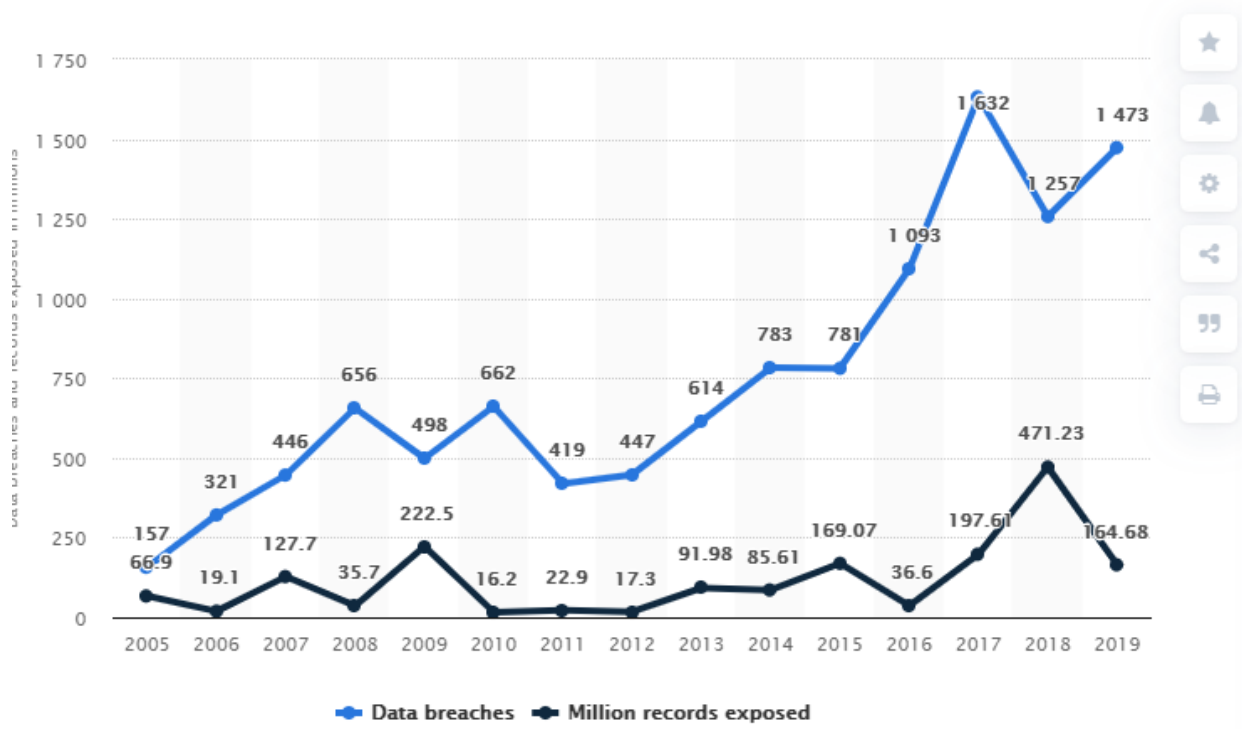


The number of PDBNs from six non-GDPR countries shows increases both from 2017 to 2018 and from 2018 to 2019. Data for four countries are above the cut-off value. One country experienced more than a 300% increase from the 2017 to 2018 fiscal year and more than a 100% increase from the 2018 to 2019 fiscal year. This country had separately reported numbers of PDBNs based on both mandatory and voluntary PDBN reporting schemes. The increase is mainly driven by mandatory PDBN reporting. The other three countries experienced a 30-50% increase from 2017 to 2018 and from 2018 to 2019.

Canada reported the number of PDBNs separately for private and public sectors. The larger increase from 2018 to 2019 is to be attributed to the private sector, for which mandatory PDBN reporting was introduced in 2018. New Zealand and Japan experienced an increase in PDBNs under a voluntary PDBN reporting arrangement. In Mexico and Turkey, while PDBN numbers are below the cut-off value, they also showed constant increase.

Data from four of the US states are above the cut-off value for all reference periods, while data from another three states are above the cut-off point for two reference periods. Data for all these states show an increase from 2017 to 2018 and a decrease from 2018 to 2019. This tendency may reflect a general increase trend from 2017 to 2018, as well as the influence of a shorter data collection period in 2019. This variation looks consistent with the trend captured by statista (Figure 15). It shows a general increase in data breaches but a plateau from 2017 to 2019 in the United States, which has several years of breach reporting experience.

Figure 15. Annual number of data breaches and exposed records in the United States, 2005-09



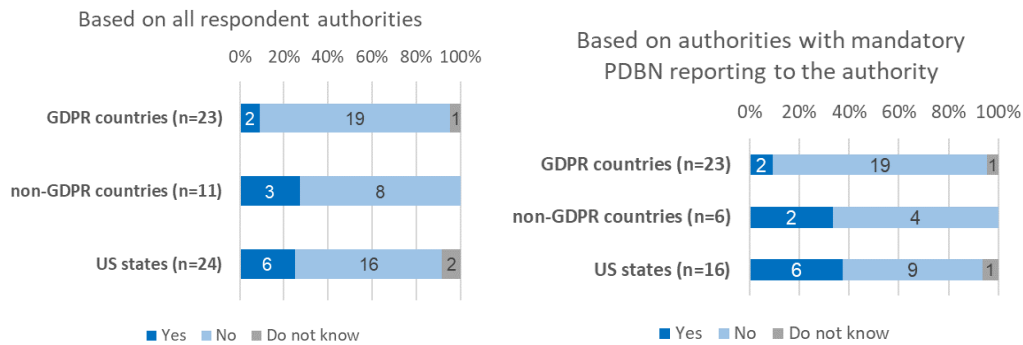
Source: Statista, available [here](#).

The survey also aimed to collect information on the number of notifications to the data subjects (QE2b). Only 5 of 23 GDPR countries, and 2 of 6 non-GDPR countries replied to the question. For the former countries, the proportion of PDBNs notified to data subjects ranges between 30% and 100%. Of the two non-GDPR countries, one reported the same number of PDBNs reported to the relevant authority; the regulation requires to notify both the authority and data subjects affected. The second country reported the number of PDBNs for the public and private sectors separately. The proportion of PDBNs that is also notified to data subjects ranges between 66% and 90% for public sector and 29% and 75% for the private sector.

Ten of 14 US states provided the number of PDBNs that are also notified to data subjects. All ten states reported exactly the same number of PDBNs in questions QE2b, (which asks respondents for the number of PDBNs also reported to data subjects) and QE2a (which asks respondents for the number of PDBNs reported to the authorities).

Two of 23 GDPR countries, 3 of 11 non-GDPR countries and 6 of 24 US states reported they record the total number of individuals affected by data breaches in their most recent reference period (QE3). When focusing on authorities with mandatory PDBN reporting, the proportion of authorities recording the number of affected individuals changes slightly (Figure 16).

Figure 16. Proportion of authorities that recorded the total number of individuals that were affected in 2017 through 2019 (QE3)

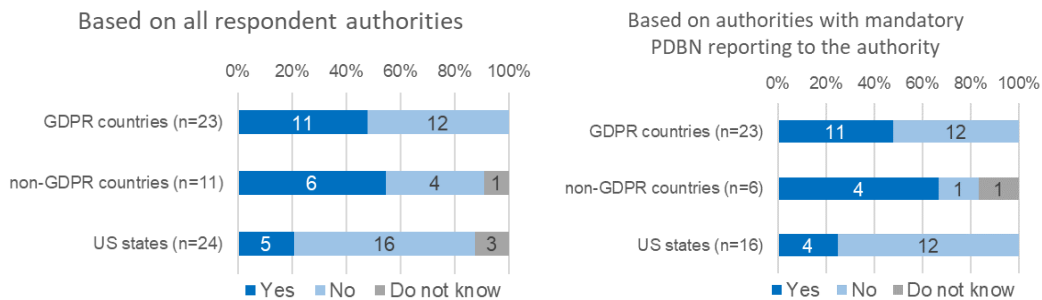


Answers to the subsequent question on the total number of individuals affected in the most recent reference periods varied significantly. Some authorities reported approximate numbers, while others provided exact numbers. However, according to one respondent, these numbers reflected only reported cases particularly under voluntary arrangements. Some US states noted this information is available publicly but that compilation may be time-consuming.

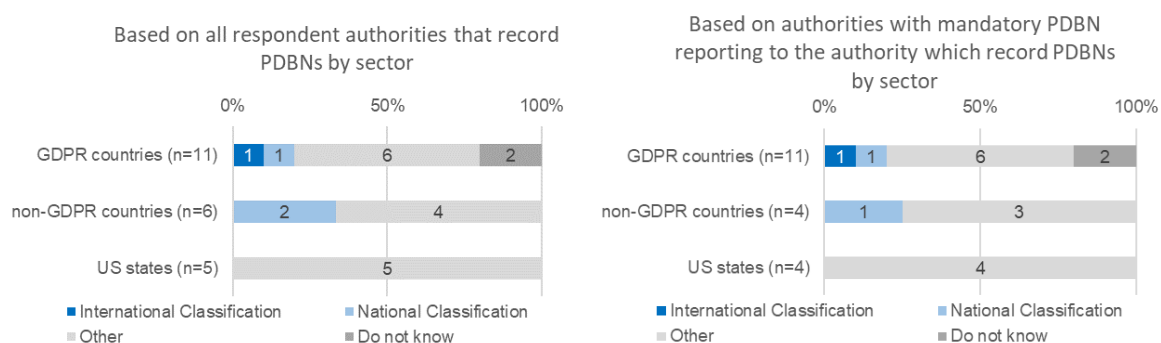
F. Personal data breach notification by sector

Eleven of 23 GDPR countries, 6 of 11 non-GDPR countries and 5 of 24 US states answered they record PDBNs by sector (QF1). These numbers are slightly higher for authorities with mandatory PDBN (Figure 17).

Figure 17. Proportion of authorities that recorded PDBNs by sector in which breaches occur (QF1)



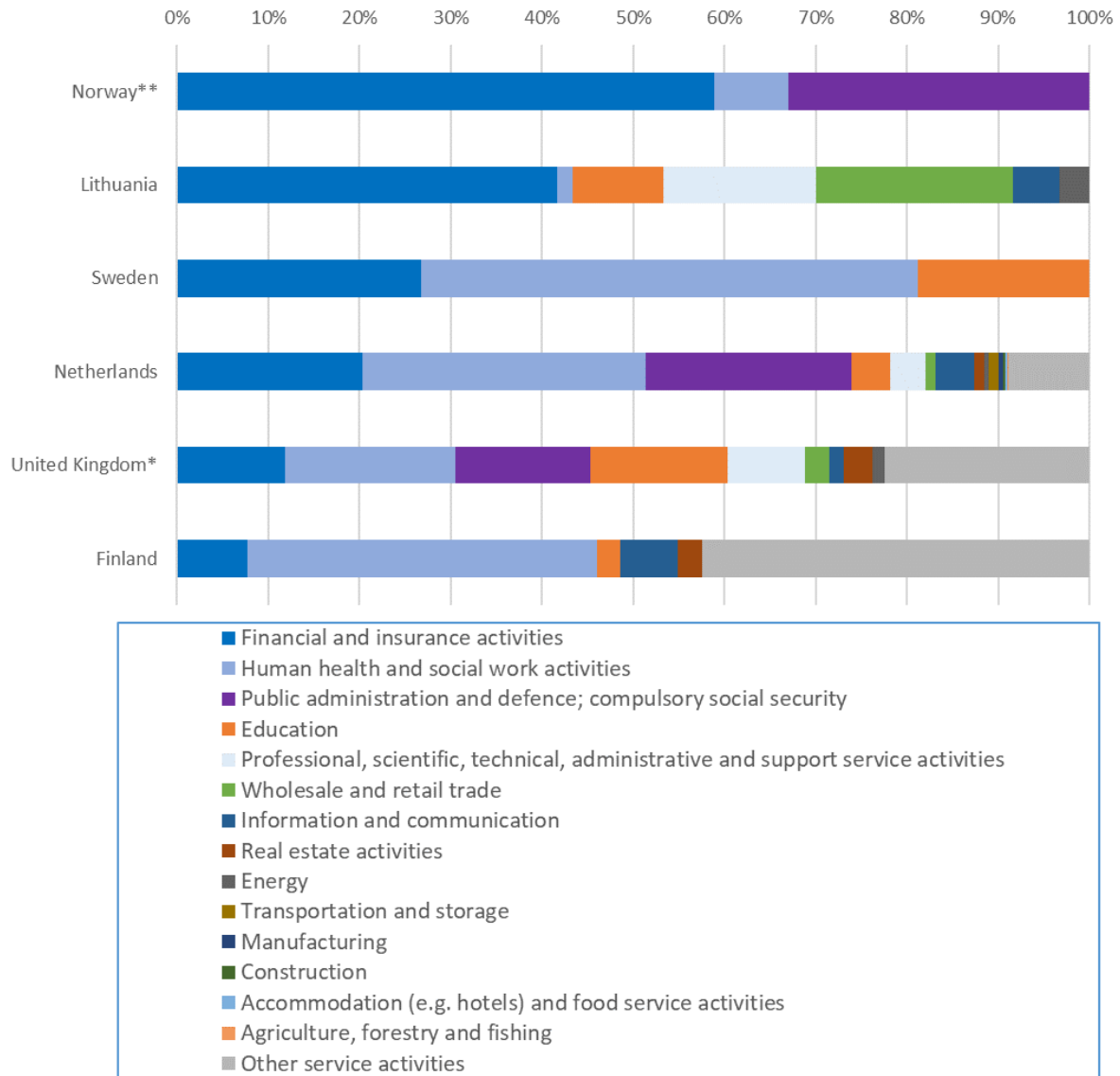
With respect to QF3, only one GDPR country reported using an international classification, while another GDPR country and two non-GDPR countries used their national industrial classifications. Most (6 of 11 GDPR countries, 4 of 6 non-GDPR countries and all 5 US states) chose “other” and answered they used their own classifications. Restricting the analysis to the authorities with mandatory PDBNs does not change this tendency (Figure 18). This use of different classification systems would naturally impact the international comparability of the EU-wide and US-wide PDBN statistics for this question.

Figure 18. Industrial classifications used to report on PDBNs by sector (QF3)

Six GDPR countries, four non-GDPR countries and four US states provided the number of PDBNs by sector according to the International Standard Industrial Classification of all Economic Activities (ISIC) (QF4). Sectors in which PDBNs are reported may depend on a number of factors such as PDBN reporting regulations, industrial structure and classification used. Data presented here only aim to shed light on a possible common sectoral PDBN trend.

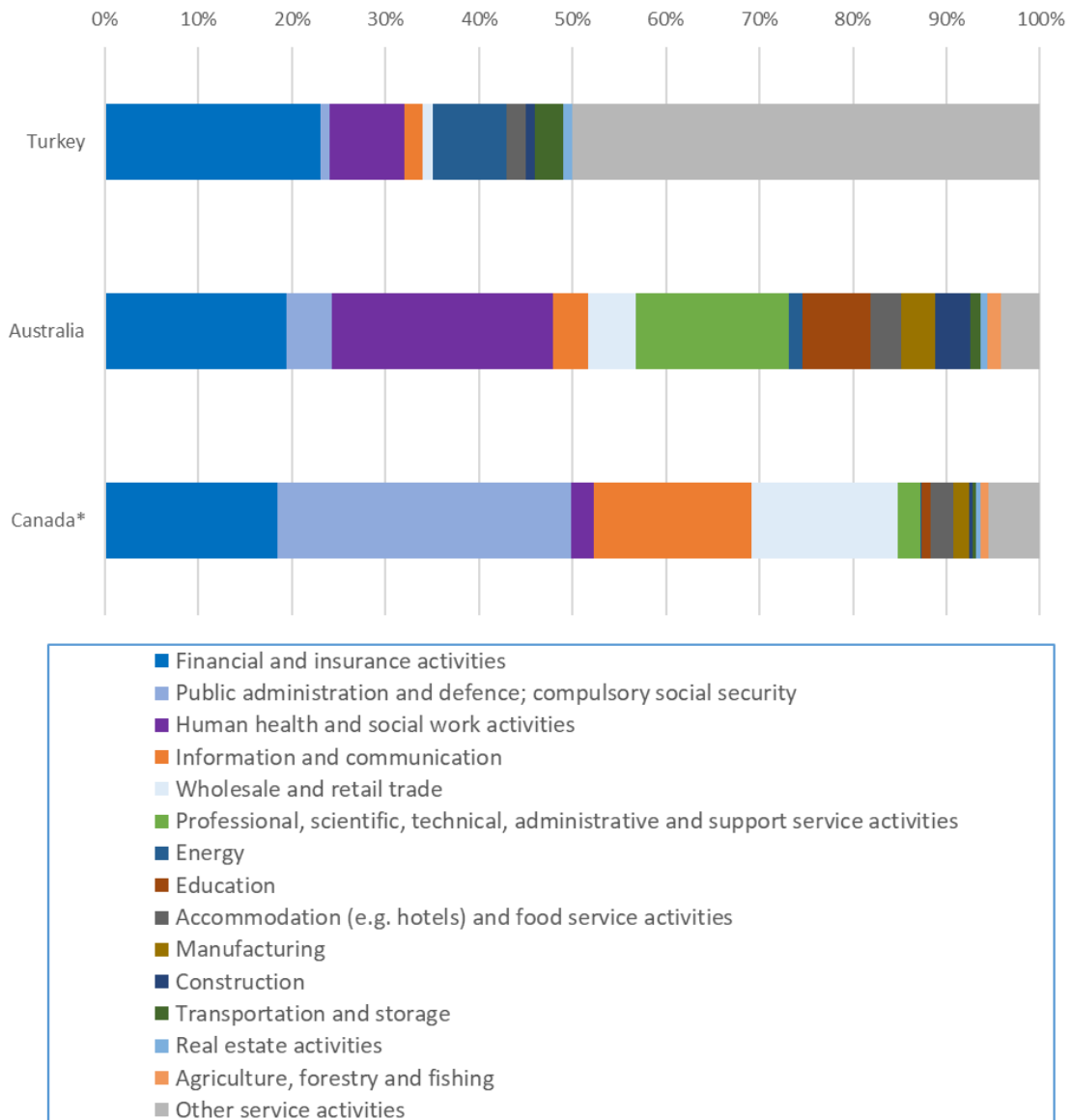
Two GDPR countries provided the number of PDBNs for all sectors, while the remaining three GDPR countries provided numbers only for some sectors. Figure 19 shows the proportion of PDBNs by sector in the six countries. Figure 20 shows the proportion of PDBNs by sector for three non-GDPR countries in 2019 (the number of one non-GDPR country is smaller than the cut-off value). Two of the four US states provided the number of PDBNs above the cut-off. Based on the same methodology, the top sectors for these two US states are “Financial and insurance activities”, “Human health and social work activities” and “Professional, scientific, technical, administrative and support service activities”, closely followed by “Education”. In sum, “Financial and insurance activities” and “Human health and social work activities” are commonly listed in top sectors subject to PDBN among GDPR and non-GDPR countries but also in the US states.

Figure 19. Proportion of PDBNs by sector in six GDPR countries in 2019 (QF4)



Note: * Refers to countries reporting according to fiscal years. ** Refers to countries providing approximate values for Financial and insurance activities between 2016 and 2018.

Figure 20. Proportion of PDBNs by sector for three non-GDPR countries in 2019 (QF4)

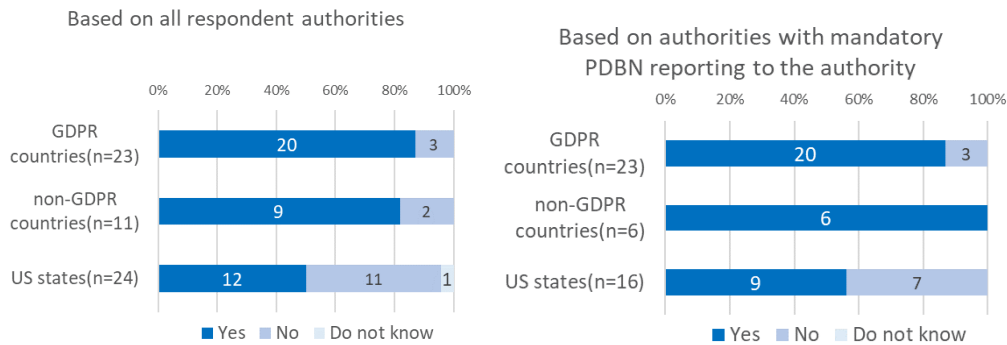


Note: * Refers to countries separately providing values of public and private sector for “Public administration and defence; compulsory social security”, which are combined in the figure.

G. Nature and type of personal data breach incident

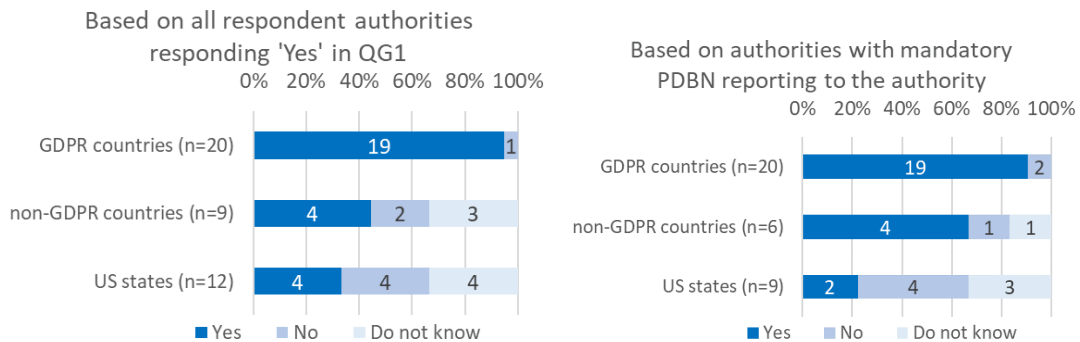
Twenty of 23 GDPR countries, 9 of 11 non-GDPR countries and 12 of 24 US states collect information on the nature and types of personal data breach incidents (QG1). These numbers are higher when the analysis is restricted to authorities with mandatory PDBN reporting to the authority (Figure 21). Since QG1 is a screening question for QG2 and QG3, the analysis of answers to these questions is based on authorities that answered “Yes” to QG1. Meanwhile, the analysis of answers to QG4 and QG8 is based on all the respondents because they were asked to all the respondents, irrespective of answer in QG1.

Figure 21. Proportion of authorities that collect information on the nature and types of personal data breach incidents (QG1)



The questionnaire also sought to determine whether it is possible to classify PDBN data by type of breach, namely availability breach, integrity breach and/or confidentiality breach (QG2). All but one of the 20 GDPR countries, 4 of 9 non-GDPR countries and 4 US states answered it is possible to classify their PDBN data in this way. Restricting analysis to authorities with mandatory PDBN reporting to the authority does not much change the proportion of authorities that answered “Yes” to the question (Figure 22).

Figure 22. Proportion of authorities that can classify PDBNs into availability, integrity and confidentiality breaches (QG2)



As to the nature and causes of breach incidents, more than 60% of respondents answered it is possible to classify PDBNs in their jurisdictions by “malicious or non-malicious”, “internal or external” and “human error” (QG3) (Table 9).

Table 9. Proportion of authorities that answered it is possible to classify personal data breaches by nature of causes (QG3)

Based on all respondent authorities responding “Yes” in QG1

| | GDPR countries(n=20) | non-GDPR countries(n=9) | US states (n=12) |
|----------------------------|----------------------|-------------------------|------------------|
| Malicious or non-malicious | 16 (80%) | 6 (67%) | 7 (55%) |
| Internal or external | 16 (80%) | 6 (67%) | 9 (75%) |
| Human error | 13 (65%) | 6 (67%) | 9 (75%) |
| Non-digital processes | 13 (65%) | 5 (56%) | 4 (33%) |
| Cross-border | 18 (90%) | 4 (44%) | 4 (33%) |

Based on authorities with mandatory PDBN reporting to the authority

| | GDPR countries(n=20) | non-GDPR countries(n=6) | US states (n=9) |
|----------------------------|----------------------|-------------------------|-----------------|
| Malicious or non-malicious | 16 (80%) | 5 (83%) | 5 (56%) |
| Internal or external | 16 (80%) | 5 (83%) | 7 (78%) |
| Human error | 13 (65%) | 5 (83%) | 7 (78%) |
| Non-digital processes | 13 (65%) | 4 (67%) | 3 (33%) |
| Cross-border | 18 (90%) | 3 (40%) | 3 (33%) |

Separately, respondents were also asked if the authority collects information on “near misses” of personal data breaches (QG4). Only one GDPR country, one non-GDPR country and two US states answered they do. The GDPR country indicated they have received “near miss reports” when data controllers voluntarily report this information but that the authority does not store such reports. The non-GDPR country noted that reporting on near misses is rare. On the other hand, one of the two US states collects information on near misses when the authority investigates breaches and finds that personal information has not been compromised.

The last question in this section (QG8) investigated whether it is possible to classify PDBNs into eight specific sub-categories (listed in Table 10), irrespective of the answers to QG1. More than 50% of GDPR countries and around 40% of the US states use all the proposed sub-categories of causes of PDBNs. More than 60% of non-GDPR countries use seven of the eight sub-categories. Respondents with a mandatory PDBN reporting have higher proportions of authorities where these proposed sub-categories are used (Table 10).

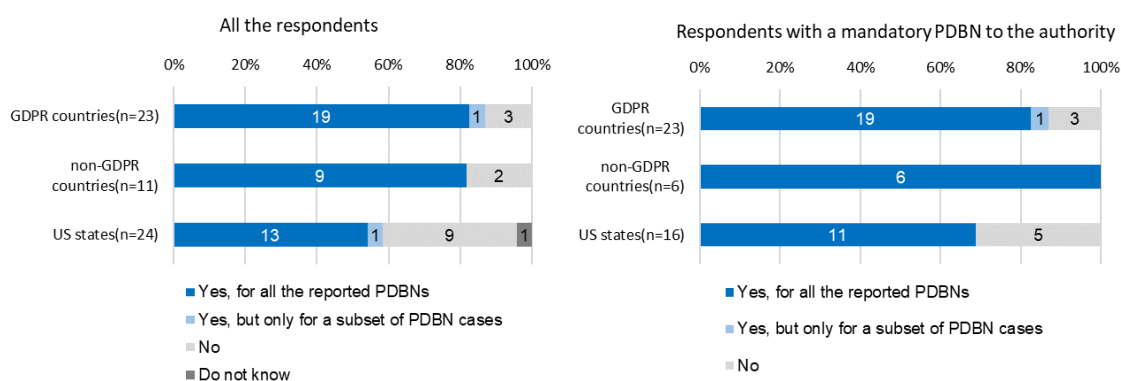
Table 10. Proportion of authorities that answered it is possible to classify the PDBN data into specific sub-categories (QG8)

| Based on all respondent authorities | | | |
|-------------------------------------|----------------------|--------------------------|------------------|
| | GDPR countries(n=23) | non-GDPR countries(n=11) | US states (n=24) |
| Loss of IT equipment | 17 (74%) | 8 (73%) | 11 (46%) |
| Mailing | 17 (74%) | 8 (73%) | 10 (42%) |
| Hacking | 17 (74%) | 7 (64%) | 10 (42%) |
| Technical error | 16 (70%) | 8 (73%) | 9 (38%) |
| Theft | 16 (70%) | 8 (73%) | 10 (42%) |
| Improper disposal of documents | 15 (65%) | 8 (73%) | 9 (38%) |
| Unauthorised access | 14 (61%) | 9 (82%) | 10 (42%) |
| Unauthorised disclosure | 12 (52%) | 4 (36%) | 10 (42%) |
| Other | 9 (39%) | 2 (18%) | 3 (13%) |

| Based on authorities with mandatory PDBN reporting to the authority | | | |
|---|----------------------|-------------------------|------------------|
| | GDPR countries(n=23) | non-GDPR countries(n=6) | US states (n=16) |
| Loss of IT equipment | 17 (74%) | 6 (100%) | 9 (56%) |
| Mailing | 17 (74%) | 6 (100%) | 8 (50%) |
| Hacking | 17 (74%) | 6 (100%) | 8 (50%) |
| Technical error | 16 (70%) | 6 (100%) | 7 (44%) |
| Theft | 16 (70%) | 6 (100%) | 8 (50%) |
| Improper disposal of documents | 15 (65%) | 6 (100%) | 7 (44%) |
| Unauthorised access | 14 (61%) | 6 (100%) | 8 (50%) |
| Unauthorised disclosure | 12 (52%) | 3 (50%) | 8 (50%) |
| Other | 9 (39%) | 1 (20%) | 3 (19%) |

H. Types of personal data affected

Section H of the questionnaire related to the types of personal data affected by breaches. All but 3 of 23 GDPR countries (83%), 9 of 11 non-GDPR countries (82%) and 14 of 24 US states (54%) answered they collect information on the types of personal data breached, at least for a subset of their PDBN data (QH1). Authorities with mandatory PDBN reporting to the authority were more likely to collect this information (Figure 23).

Figure 23. Proportion of authorities that answered they collect information on the types of personal data breached (QH1)


Respondents who answered they do collect data on the type of personal data breached were asked whether that data could be classified as personal credential, sensitive, behavioural and/or financial (QH2). Over 65% of GDPR countries could classify the data according to these four categories. More than 50% of non-GDPR countries and more than 50% of reporting US states collect “Personal credential data”, “sensitive data” and “financial data”. Authorities with mandatory PDBN reporting to the authority are more likely to collect this information (Table 11).

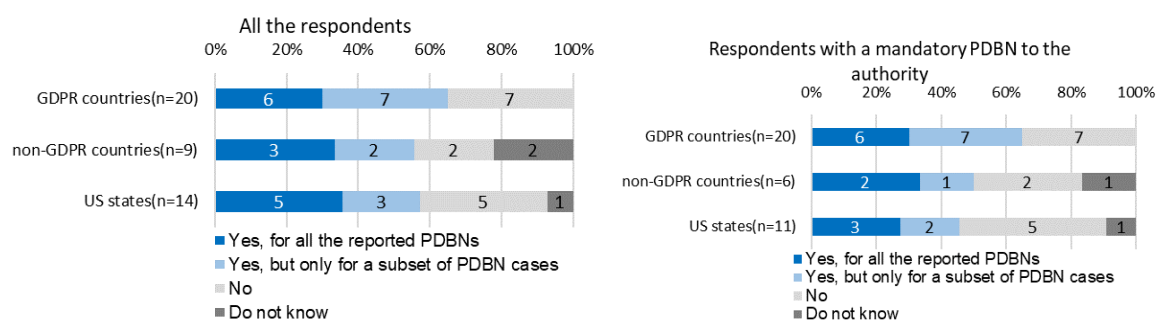
Table 11. Proportion of authorities that said they can classify PDBN data that are collected into the following sub-categories (QH2)

| All the respondents | | | |
|--------------------------|----------------------|-------------------------|------------------|
| | GDPR countries(n=20) | non-GDPR countries(n=9) | US states (n=14) |
| Personal credential data | 17 (85%) | 5 (56%) | 10 (71%) |
| Sensitive data | 16 (80%) | 6 (67%) | 7 (50%) |
| Behavioural data | 13 (65%) | 3 (33%) | 5 (36%) |
| Financial data | 16 (80%) | 5 (56%) | 11 (79%) |
| Other | 5 (25%) | 4 (44%) | 1 (7%) |

| Based on authorities with mandatory PDBN reporting to the authority | | | |
|---|----------------------|-------------------------|------------------|
| | GDPR countries(n=20) | non-GDPR countries(n=6) | US states (n=11) |
| Personal credential data | 17 (85%) | 4 (67%) | 9 (82%) |
| Sensitive data | 16 (80%) | 5 (83%) | 6 (55%) |
| Behavioural data | 13 (65%) | 2 (33%) | 4 (36%) |
| Financial data | 16 (80%) | 4 (67%) | 10 (91%) |
| Other | 5 (25%) | 4 (87%) | 1 (9%) |

The same subgroup of respondents were also asked whether they collect information on the encryption of personal data (QH3). Thirteen of 20 GDPR countries (65%), 5 of 9 non-GDPR countries (56%) and 8 of 14 US states (57%) answered they do at least for a subset of PDBNs (Figure 24).

Figure 24. Proportion of authorities that answered they collect information on encryption of personal data breached (QH3)



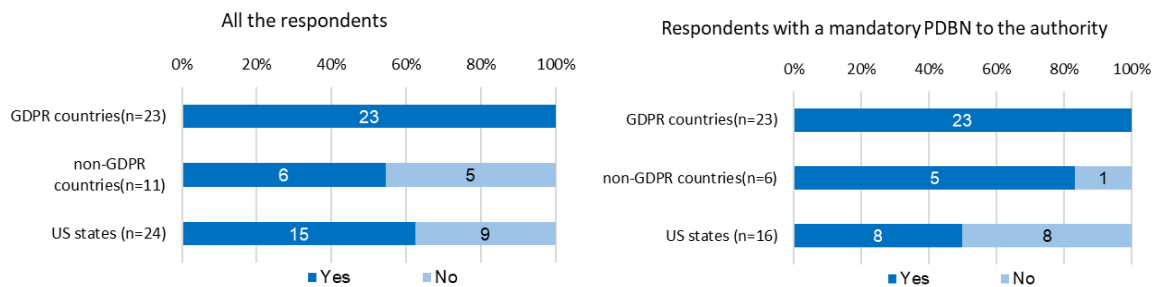
I. Monetary fines and other penalties

The questionnaire also asked countries about the regulatory actions available to respondent authorities, such as fines and investigations of personal data breaches. All the GDPR countries, 6 of 11 non-GDPR countries and 15 of 24 US states answered that fines for personal data breaches are administrated in their

jurisdictions (Q11). Respondents in non-GDPR countries with a mandatory PDBN reporting to the authority are more likely to administer fines (Figure 25).

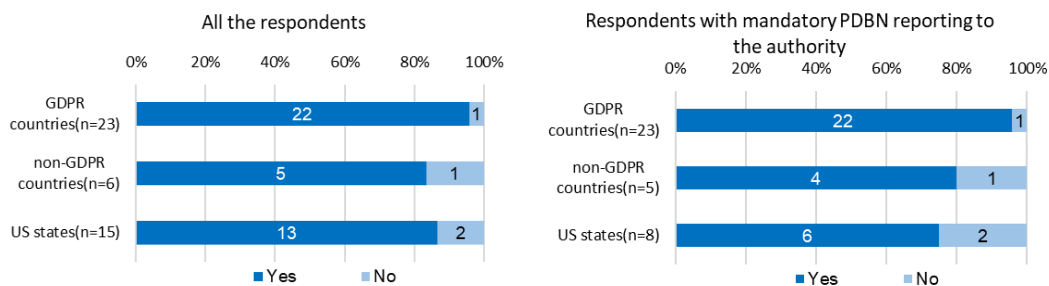
One respondent noted the question is not clear whether the regulation allows for fines or whether fines have actually been issued. Therefore, some respondents with a regulation allowing for fines might have answered “No” at Q11 by interpreting the question had asked if fines have been actually issued. It was also noted the court rather than regulators may order a financial penalty, plus there may be private litigations resulting in financial penalty on breached firms. Furthermore, there may be regulatory actions at both central and provincial levels. In fact, financial penalties on breached firms are levied as civil penalties and thus administered by courts in the United States. In addition to regulation of PDBN at the state level, other significant actions include investigations by the Federal Trade Commission (FTC), as well as private litigation in the United States. For example, the FTC settlement with Equifax following its breach required Equifax to pay between \$575-\$700 million.²³ In a private class action settlement, Equifax agreed to pay \$1.4 billion.²⁴ In another example of a private litigation settlement, Yahoo agreed to pay \$117.5 million into a settlement fund.²⁵

Figure 25. Proportion of authorities that answered fines are administered for personal data breaches in their jurisdictions (Q11)



Almost all countries that issue fines for personal data breaches explained that the respondent authority administers those fines (Q13, Figure 26). One GDPR country and another non-GDPR country indicated that other authorities are responsible for administering fines. Some US states mentioned fines are levied as civil penalties and thus administered by courts.

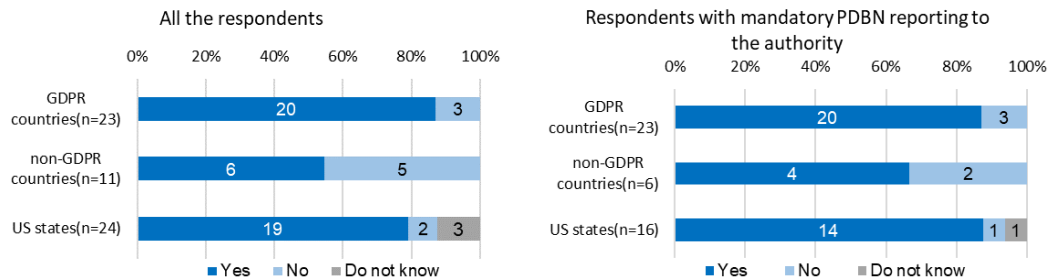
Figure 26. Proportion of authorities responsible for administering fines (Q13)



Respondents were also asked if there are any other regulatory actions taken in response to a PDBN (or lack of breach notification), which would include imposing other requirements upon the reporting organisation (Q14). Twenty of 23 GDPR countries, 6 of 11 non-GDPR countries and 19 of 24 US states answered there are other regulatory actions (Figure 27). GDPR countries referred to orders to stop the destruction of data, reduce retention, stop processing, improve digital security measures, require notification to data subjects and other actions possible under Article 58 (2) of the GDPR. Non-GDPR countries also mentioned in general that they impose necessary orders or penalties when breached

organisations do not comply with regulations after the investigation. Similarly, the US states indicated injunctive and therapeutic relief in addition to restitution and/or monetary penalties as the most frequent regulatory actions taken after investigations.

Figure 27. Proportion of authorities that can impose regulatory actions other than a fine in response to a PDBN or lack of breach notification (Q14)



Respondents were also asked about the sources of information that trigger authorities to initiate their audits/investigations (Q15). More than 50% of all respondents answered that their audits or investigations are triggered by “report from breached data controllers”, “information from affected data subjects”, “information from other authorities”, and/or “information related to personal data breaches in the media”. A good proportion (above 45%) of the GDPR and non-GDPR countries also answered other triggers include “detection of PDBN by your authority” and “information about personal data breach shared from non-affected individuals” (Table 12).

Table 12. Proportion of authorities that answered they initiated audits/investigations in response to the following sources of information (Q15)

| All respondents | | | |
|---|----------------------|--------------------------|------------------|
| | GDPR countries(n=23) | non-GDPR countries(n=11) | US states (n=24) |
| Reported PDBNs by data controllers | 21 (91%) | 9 (82%) | 17 (71%) |
| Information from influenced data subjects | 21 (91%) | 7 (64%) | 12 (50%) |
| Information from other public authorities | 13 (57%) | 5 (45%) | 17 (71%) |
| Information from other private and public bodies | 13 (57%) | 3 (27%) | 11 (46%) |
| Information related to personal data breaches in the media | 18 (78%) | 9 (82%) | 18 (75%) |
| Detection of PDBN by your authority | 13 (57%) | 8 (73%) | 6 (25%) |
| Information about personal data breach shared from non-affected individuals | 14 (61%) | 5 (45%) | 7 (29%) |
| Other | 1 (4%) | 0% | 2 (8%) |

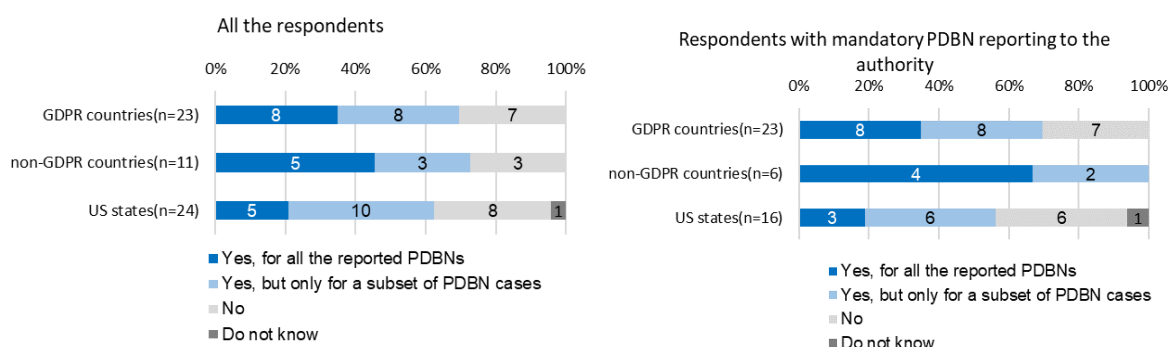
Respondents with mandatory PDBN reporting to the authority

| | GDPR countries(n=23) | non-GDPR countries(n=6) | US states (n=16) |
|---|----------------------|-------------------------|------------------|
| Reported PDBNs by data controllers | 21 (91%) | 5 (83%) | 13 (81%) |
| Information from influenced data subjects | 21 (91%) | 5 (83%) | 11 (69%) |
| Information from other public authorities | 13 (57%) | 3 (50%) | 12 (75%) |
| Information from other private and public bodies | 13 (57%) | 1 (17%) | 8 (50%) |
| Information related to personal data breaches in the media | 18 (78%) | 6 (100%) | 13 (81%) |
| Detection of PDBN by your authority | 13 (57%) | 6 (100%) | 3 (19%) |
| Information about personal data breach shared from non-affected individuals | 14 (61%) | 3 (50%) | 4 (25%) |
| Other | 1 (4%) | 0% | 1 (6%) |

J. Measures taken to prevent or mitigate risk and evaluating PDBN impacts

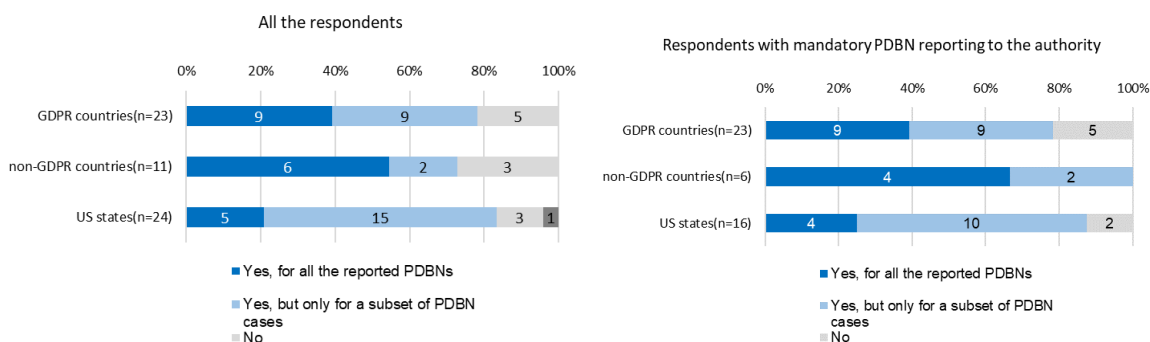
The question QJ1 related to the verification of the authenticity of the reported PDBNs. Sixteen of 23 GDPR countries (70%), 8 of 11 non-GDPR countries (73%) and 15 of 24 US states (63%) answered that authorities verify the authenticity for at least a subset of PDBNs. All respondents with a mandatory PDBN reporting to the authority in non-GDPR countries answered they do so (Figure 28). Respondents generally indicated the authenticity of PDBNs is checked when reported information needs clarification or when cases pose a risk to human rights, are of a significant magnitude, and when circumstances of the breach suggest it would be useful.

Figure 28. Proportion of authorities that answered they verify the authenticity of reported PDBNs (QJ1)



Respondents were also asked if they investigate the organisational and technical measures of the breached organisation before the reported data breach happened (QJ2). Eighteen of 23 GDPR countries (78%), 8 of 11 non-GDPR countries (73%) and 20 of 24 US states (83%) answered they do so at least for a subset of PDBNs. A higher proportion of authorities with a mandatory PDBN reporting answered they do so as well (Figure 29). The reasons triggering such an investigation only for a subset of PDBNs are similar to those reported in the question QJ1 above (risk to human rights, significant magnitude and general circumstances).

Figure 29. Proportion of authorities that investigate organisational and technical measures of the breached organisation before the data breach (QJ2)



The questionnaire also asked respondents whether they investigate the economic and social impacts of personal data breaches (QJ3). Only a few authorities in GDPR and non-GDPR countries answered they do so, as opposed to half of the US states (Figure 30). Table 13 shows the proportion of authorities that investigate the proposed factors of economic and social impacts on the organisation that reported a personal data breach.

Figure 30. Proportion of authorities that answered they investigate the economic and social impacts on the organisation that reported a personal data breach (QJ3)

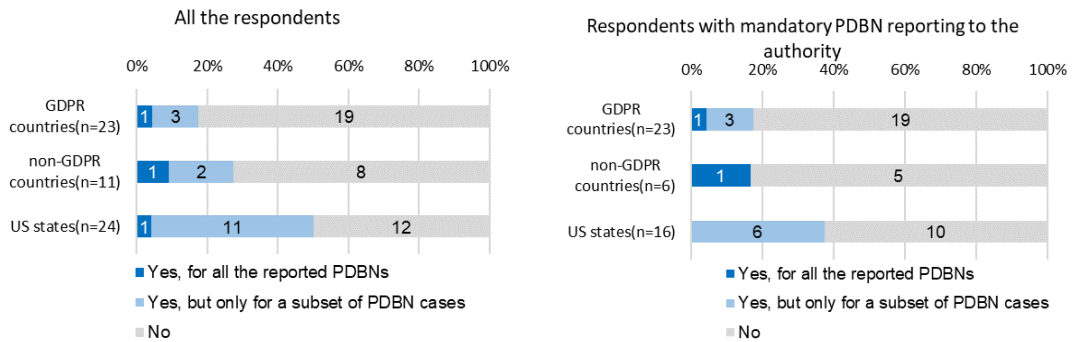


Table 13. Proportion of authorities that investigate various economic and social impacts on the organisation that reported a PDBN (QJ3)

| | All respondents | | |
|---|----------------------|--------------------------|------------------|
| | GDPR countries (n=4) | non-GDPR countries (n=3) | US states (n=12) |
| Technical investigation and recovery activity | 3 (75%) | 3 (100%) | 11 (92%) |
| Improvement of digital security | 3 (75%) | 3 (100%) | 11 (92%) |
| Loss of monetary value that otherwise breached personal data would create | 2 (50%) | 1 (33%) | 7 (58%) |
| Private litigation with stakeholders | 1 (25%) | 1 (33%) | 8 (67%) |
| Fines and regulatory requirements | 2 (50%) | 2 (67%) | 12 (100%) |
| Disrupted operation | 2 (50%) | 1 (33%) | 7 (58%) |
| Public relations | 1 (25%) | 2 (67%) | 10 (83%) |
| Activity to keep current customers | 0 | 1 (33%) | 6 (50%) |
| Loss of revenue | 2 (50%) | 0 | 5 (42%) |
| Loss of customer base | 2 (50%) | 0 | 4 (33%) |
| Change in stock price | 2 (50%) | 0 | 6 (50%) |
| Increase in insurance premium and debt raising | 2 (50%) | 0 | 3 (25%) |
| Other | 1 (25%) | 0 | 1 (8%) |

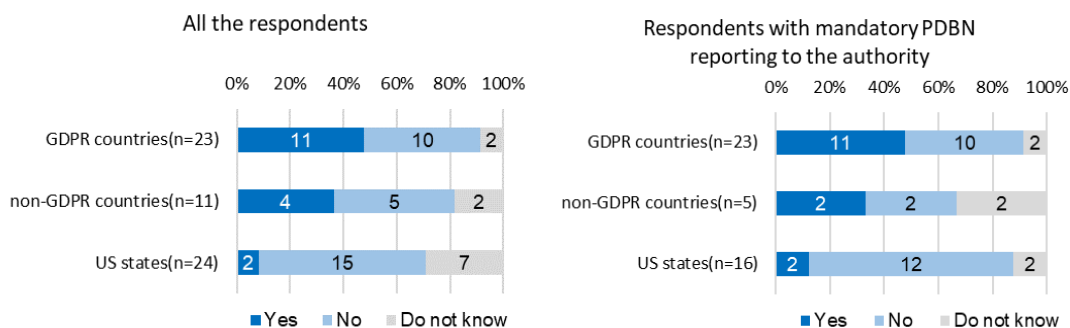
Respondents with mandatory PDBN reporting to the authority

| | GDPR countries(n=4) | non-GDPR countries(n=1) | US states (n=6) |
|---|---------------------|-------------------------|-----------------|
| Technical investigation and recovery activity | 3 (75%) | 1 (100%) | 6 (100%) |
| Improvement of digital security | 3 (75%) | 1 (100%) | 6 (100%) |
| Loss of monetary value that otherwise breached personal data would create | 2 (50%) | 0 | 4 (67%) |
| Private litigation with stakeholders | 1 (25%) | 0 | 5 (83%) |
| Fines and regulatory requirements | 2 (50%) | 0 | 6(100%) |
| Disrupted operation | 2 (50%) | 1 (100%) | 3 (50%) |
| Public relations | 1 (25%) | 0 | 5 (83%) |
| Activity to keep current customers | 0 | 0 | 2 (33%) |
| Loss of revenue | 2 (50%) | 0 | 2 (33%) |
| Loss of customer base | 2 (50%) | 0 | 2 (33%) |
| Change in stock price | 2 (50%) | 0 | 2 (33%) |
| Increase in insurance premium and debt raising | 2 (50%) | 0 | 1 (17%) |
| Other | 1 (25%) | 0 | 0 (8%) |

K. Use of PDBN data

Section K of the questionnaire sought to collect information on the use of PDBN data collected by authorities. Eleven of 23 GDPR countries, 4 of 11 non-GDPR countries and 2 of 24 US states said they use the data for budget planning for the next year and improving operations within the authority (QK1). Respondents with mandatory PDBN reporting to the authority show comparable ratios (Figure 31). Respondents indicated the number of PDBNs, investigations and penalties feed into planning for strategic priorities and resources such as budget allocation and employment decisions. This implies the question should address broader use of PDBN data for planning.

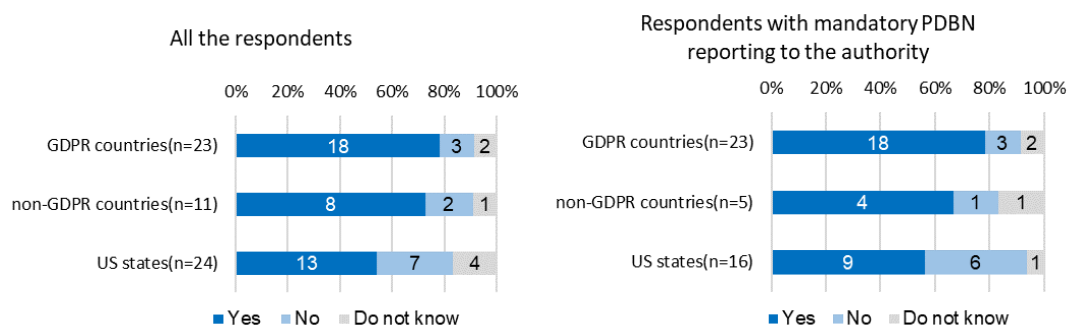
Figure 31. Proportion of authorities that answered they use the PDBN data for budget planning for the next year and improving operation within the authority (QK1)



More than half of respondents answered they use PDBN data for improving public relations to raise awareness of targeted sectors and entities (such as small and medium-sized enterprises) and certain risks (QK2). This figure changes little when analysis is limited to respondents with mandatory PDBN reporting

to the authority (Figure 32). Some respondents also specified activities to raise awareness. Specifically, some authorities issue recommendations and guidance on how to improve security and protect personal data in the event of a breach. They supplement this information with data revealing regular patterns of breaches, statistics and anonymous case studies. Authorities also share this information through press releases and reports on their websites; events with stakeholders such as businesses and other target groups; and educational materials and collaboration with local media.

Figure 32. Proportion of authorities that use PDBN data for improving public relations to raise awareness of targeted sectors and entities and certain risks (QK2)



In addition, more than 50% of GDPR and non-GDPR countries and around 30% of the US states reported that their authority uses the PDBN data to improve guidelines for data controllers regarding appropriate organisational measures, technical measures on digital processes and technical measures on physical environments (QK3). These percentages were higher among respondents with mandatory PDBN (Table 14). PEAs have tried to help organisations comply with PDBN regulations, including via digital tools such as a web form created by the Spanish PEA to help them decide whether to notify data subjects.²⁶ Consequently, the scope of QK3 should be expanded.

Table 14. Proportion of authorities that use PDBN data for improving specific guidelines that data controllers are required to implement (QK3)

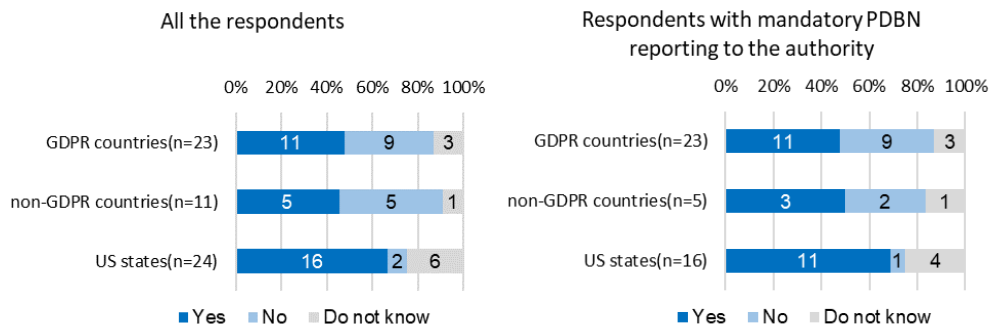
| | All respondents | | |
|--|-----------------------|---------------------------|------------------|
| | GDPR countries (n=23) | non-GDPR countries (n=11) | US states (n=24) |
| Organisational measures | 17 (74%) | 6 (55%) | 6 (25%) |
| Technical measures on digital processes | 15 (65%) | 7 (64%) | 7 (29%) |
| Technical measures on physical environment | 14 (61%) | 6 (55%) | 7 (29%) |
| Other | 1 (4%) | 0 | 2 (8%) |

Respondents with mandatory PDBN reporting to the authority

| | GDPR countries(n=23) | non-GDPR countries(n=6) | US states (n=16) |
|--|----------------------|-------------------------|------------------|
| Organisational measures | 17 (74%) | 4 (67%) | 5 (31%) |
| Technical measures on digital processes | 15 (65%) | 4 (67%) | 6 (38%) |
| Technical measures on physical environment | 14 (61%) | 4 (67%) | 6 (38%) |
| Other | 1 (4%) | 0 | 2 (13%) |

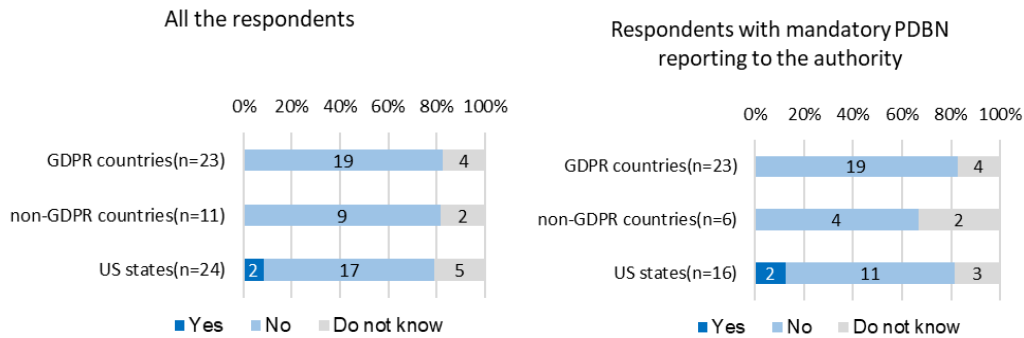
The questionnaire also collected information on the use of PDBN data to reinforce the collaboration with other authorities responsible for digital security, consumer policy, law enforcement and other related areas (QK4). Eleven of 23 GDPR countries, 5 of 11 non-GDPR countries and 16 of 24 US states answered they use PDBN data for these purposes (Figure 33). Organisations mentioned as partners include digital security agencies, national Computer Emergency Response Teams (CERTs), ministries of education, law enforcement authorities, consumer policy agencies and sectoral regulatory authorities of health, transport and telecommunication. Some GDPR countries also mentioned collaboration with non-EU countries, and some US states referred to multistate collaborations.

Figure 33. Proportion of authorities that use PDBN data for reinforcing collaboration with other authorities responsible for digital security, consumer policy, law enforcement, etc. (QK4)



Finally, respondents were asked whether they use PDBN data to evaluate the economic impacts of personal data breaches within their jurisdiction or their geographical scope (QK5). Only two US states provided a positive answer to this question (Figure 34). One state indicated that it may consider economic impact to determine appropriate restitution awards and civil penalties. The other explained it only gathers information about state-specific impacts of a personal data breach after the authority opens or joins an investigation.

Figure 34. Proportion of authorities that use PDBN data to evaluate the economic impacts of personal data breaches within their jurisdiction or their geographical scope (QK5)



L. Summary of potentially workable questions

This survey provides evidence on the type of questions that are suitable for the ongoing PDBN data collection by PEAs. It also suggests which questions need revision to collect internationally comparable metrics on PDBNs. Table 15 summarises potentially workable questions to achieve this purpose. Questions with a low response rate are not presented.

The questionnaire included under Annex A is a modified version based on the analysis and suggestions by both DGP and MADE delegates. Proposals from a few respondents are left as possible additional questions depending on the context.

Table 15. Potential set of workable questions to improve comparability

| | Note |
|--|---|
| QB2 and QB3: budget and its sources | Some authorities do not have a budget allocated to PDBNs. |
| QB5a and QB5b: staff number in PEA and in a group for PDBNs | Some authorities do not assign staff to cover PDBNs. |
| QC1: mandatory requirement to report the authority | |
| QC2: sectoral application of mandatory PDBN to the authority | Some jurisdictions seem to have different criteria for when to notify individuals or the authority. |
| QC3: trigger to notify the authority | |
| QC4: timeframe to notify the authority | |
| QC5: notification to data subjects | |
| QC6: central database | Meaning of “central” should be clarified. |
| QD1: publicly available statistics | |
| QD2: data provision to OECD | |
| QE1&2: number of PDBNs | Different data collection periods should be specified. |
| QE3: total number of affected individuals | The question asking about statistical figures is not suitable to PEA data collection practices. |
| QF1: recording of PDBNs by sector | |
| QF3&4: industrial classification and sectoral number of PDBNs | Consistency must be ensured with the use of interoperable classification. |
| QG2: AIC classification of PDBNs | Not all notifications can be easily retrofitted in the AIC classification |
| QG3: nature of causes of the event | Three of five categories of proposed causes apply to most respondents |
| QG8: sub-category of causes | Five of eight proposed sub-categories apply to most respondents. |
| QH2: sub-categories of personal data | All categories but “Behavioural data” apply to most respondents. |
| QH3: encryption | |
| QI1&QI3: administration of fines | |
| QI4: other regulatory actions | |
| QI5: thresholds to initiate investigations | Four of seven proposed thresholds appear common to most respondents. |
| QJ1: verification of authenticity of PDBNs | |
| QJ2: measures taken before breaches | |
| QJ3: indicators of economic and social impacts on breached organizations | Three of 12 proposed indicators work for most respondents that answered “Yes”. |
| QK1: use of PDBN data for resource and operation planning | Question should be reworded to capture broader use of PBDN data for planning. |
| QK2: use of PDBN data for public relations | |
| QK3: use of PDBN data for improving guidelines | Respondents may need to understand the term “guidelines” better. |
| QK4: use of PDBN data for collaboration with other authorities | |

ANNEX A. Revised questionnaire

A. General questions and authority profile

QA1. Please provide the name and contact email address of the person completing this survey:

These details will not be released but will enable the OECD Secretariat to clarify responses if necessary.

| | Name | E-mail address |
|------------------|----------------------|----------------------|
| Contact details: | <input type="text"/> | <input type="text"/> |

***QA2. Please provide the name of your Privacy Enforcement Authority (PEA):**

*** QA2a. Please select your country:**

***QA3. What is the jurisdiction or geographical scope of the authority?**

- Federal/National
- Local/Provincial/State/Regional
- International/Supranational

***QA4. Is your authority involved in enforcing regulation on personal data breach notification (PDBN)?**

- Yes
- No
- Do not know

***QA5. Does your authority oversee privacy protection practices by the following sectors? (Select all that apply)**

- the public sector
- the private sector
- the non-profit sector (NPOs, charities, etc.)
- Other

***If selected Other, please specify:**

***QA6. In addition to roles under a data protection or privacy law mandate and power, does your authority perform other regulatory or oversight functions? (e.g. under the Government information access or Freedom of Information law)**

- Yes
- No
- Do not know

***If answered Yes, please specify what other regulatory or oversight functions are performed:**

B. Authority's funding and human resources

Please note: If there are more than one PEAs in your country, report information only for your own authority. If your authority is funded over a longer period than one year (e.g. 2 or 5 years), please report for all of the questions in this section funding estimates broken down by year. If your authority does not use calendar year, please specify the relevant reference periods (e.g. fiscal year) as indicated in the questions below.

B-1: FUNDING

***QB1. Are 2020, 2019 and 2018 your most recent reference periods for providing funding information?**

- Yes
- No

Any additional comments:

*** If answered No, please specify below your most recent reference periods for funding information, instead of 2020, 2019 and 2018.**

| | |
|------------------|----------------------|
| Instead of 2020: | <input type="text"/> |
| Instead of 2019: | <input type="text"/> |
| Instead of 2018: | <input type="text"/> |

***QB2. Do you know what the total budget of your authority was in 2019 (or most recent reference period)?**

- Yes
- No (go to QB4)

Any additional comments:

QB2a. If known, please specify the total budget of your authority including all sources of funding (e.g. budget allocation to your authority within the government, registration or licensing fees, chargeable services and fines and penalties).

| | Amount | Currency |
|---|----------------------|------------------------------|
| In 2020 (or reference period specified above) | <input type="text"/> | Select: <input type="text"/> |
| In 2019 (or reference period specified above) | <input type="text"/> | Select: <input type="text"/> |
| In 2018 (or reference period specified above) | <input type="text"/> | Select: <input type="text"/> |

***QB3. Does your authority’s funding in 2020 (or most recent reference period) which was answered in QB2a originate from any of the following sources?**

| | Yes | No | Do not know | If YES, percentage of total funding if known |
|---|-----------------------|-----------------------|-----------------------|--|
| Budget allocation within the government | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="text"/> |
| Registration or licensing fees | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="text"/> |
| Chargeable services (e.g. auditing, training, publications) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="text"/> |

| | | | | |
|---------------------|-----------------------|-----------------------|-----------------------|----------------------|
| Fines and penalties | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="text"/> |
| Other | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="text"/> |

*** If selected Other, please specify:**

[Additional possible question]

QBx. Do you know the budget specifically allocated to the department/division/section that deals with PDBN within your authority, including all sources of funding (e.g. budget allocation to your authority within the government, registration or licensing fees, chargeable services and fines and penalties)?

- Yes
- No

If answered Yes, please specify below.

| | Amount | Currency |
|---|----------------------|------------------------------|
| In 2020 (or reference period specified above) | <input type="text"/> | Select: <input type="text"/> |
| In 2019 (or reference period specified above) | <input type="text"/> | Select: <input type="text"/> |
| In 2018 (or reference period specified above) | <input type="text"/> | Select: <input type="text"/> |

B-2: HUMAN RESOURCES

***QB4. Are 2020, 2019 and 2018 your most recent reference periods for resource information (on the number of staff)?**

- Yes
- No

*** If answered No, please specify below your most recent reference periods for resource information (on the number of staff), instead of 2019, 2018 and 2017.**

| | |
|------------------|----------------------|
| Instead of 2020: | <input type="text"/> |
| Instead of 2019: | <input type="text"/> |
| Instead of 2018: | <input type="text"/> |

*** QB5. Do you know how much staff is employed by your authority (full time equivalent employees)?**

- Yes
- No (go to next section)

QB5a. If known, please specify the total number of staff employed (full time equivalent employees).

| | Number of staff |
|---|----------------------|
| In 2020 (or reference period specified above) | <input type="text"/> |
| In 2019 (or reference period specified above) | <input type="text"/> |
| In 2018 (or reference period specified above) | <input type="text"/> |

QB5b. If known, please specify the number of staff employed (full time equivalent employees) in the department/division/section that deals with PDBN.

| | Number of staff |
|---|----------------------|
| In 2020 (or reference period specified above) | <input type="text"/> |
| In 2019 (or reference period specified above) | <input type="text"/> |
| In 2018 (or reference period specified above) | <input type="text"/> |

C. Personal data breach notification reporting law, jurisdiction and exemptions

This section asks regulatory profiles of the personal data breach notification system for both the authority and data subjects. Subsequently, this section asks about database for received personal data breach notifications.

C-1: REPORTING TO THE AUTHORITY

***QC1. Is there a mandatory requirement to report personal data breaches to one or more enforcement authorities in your jurisdiction?**

- Yes (go to QC2)

- No (go to QC1a)
- Do not know (go to QC2)

*** If answered Yes, please specify the enforcement authority/authorities:**

***QC1a. Will PDBN reporting to the authority become mandatory in the next two years?**

- Yes, a new law or other policy requirement has been passed and will come into force within the next two years (go to QC5)
- Probably, a new law or other policy requirement is expected to be in force within the next two years (go to QC5)
- No (go to QC5)
- Do not know (go to QC5)

***QC2. Does the mandatory PDBN reporting to the enforcement authority/authorities apply generally or to particular sectors? (Select all that apply)**

- | | Year in which mandatory regulation started. |
|---|---|
| <input type="checkbox"/> Generally | <input style="width: 100%;" type="text"/> |
| <input type="checkbox"/> All public sector | <input style="width: 100%;" type="text"/> |
| <input type="checkbox"/> All private sector regardless of size | <input style="width: 100%;" type="text"/> |
| <input type="checkbox"/> All private sector with exceptions depending on size and turnover | <input style="width: 100%;" type="text"/> |
| <input type="checkbox"/> Telecommunications sector | <input style="width: 100%;" type="text"/> |
| <input type="checkbox"/> Health sector (including, for example, private hospitals, day surgeries, medical practitioners, pharmacists, allied health professionals, gyms and weight loss clinics, childcare centres, and medical services in educational institutions) | <input style="width: 100%;" type="text"/> |
| <input type="checkbox"/> Financial Sector (including, for example, banks and credit reporting bodies) | <input style="width: 100%;" type="text"/> |
| <input type="checkbox"/> Other | <input style="width: 100%;" type="text"/> |

*** If selected Other, please specify:**

If possible, provide URLs of regulatory documents such as the laws, decrees, and guidelines on PDBN:

***QC3. Which of the following aspects trigger the PDBN to the enforcement authority/authorities? (Select all that apply)**

- Any breach that poses a risk of harm to or adverse effect on the data subject
- Unauthorised access, regardless of risk of harm to or adverse effect on the data subject
- Unauthorised deletion, regardless of risk of harm to or adverse effect on the data subject
- Unauthorised alteration, regardless of risk of harm to or adverse effect on the data subject
- Unauthorised acquisition, regardless of risk of harm to or adverse effect on the data subject
- Particular types of data, regardless of risk of harm to or adverse effect on the data subject
- Any breach that involves the personal data that is not encrypted
- Scope of breach (such as the number of people impacted)
- Other

*** If selected Other, please specify:**

*** If exceptions or sector-specific requirements apply, please specify:**

***QC4. Within which timeframe is the PDBN to the enforcement authority/authorities required? (Select all that apply)**

- Within a prescribed time frame (e.g. 72 hours) where feasible
- Quickly or as soon as possible without unreasonable delay
- Other (please specify)

If exceptions apply or there are several different timeframes, please specify:



C-2: REPORTING TO DATA SUBJECTS

***QC5. Is there a mandatory requirement to report personal data breaches to data subjects in your jurisdiction?**

- Yes (go to QC6)
- No (go to QC5a)
- Do not know (go to QC6)

***QC5a. Will PDBN reporting to data subjects become mandatory in the next two years?**

- Yes, a new law or other policy requirement has been passed and will come into force within the next two years (go to QC5)
- Probably, a new law or other policy requirement is expected to be in force within the next two years (go to QC5)
- No (go to QC5)
- Do not know (go to QC5)

***QC6. Does the mandatory PDBN reporting to data subjects apply generally or to particular sectors? (Select all that apply)**

- | | |
|--|--|
| <ul style="list-style-type: none"> <input type="checkbox"/> Generally <input type="checkbox"/> All public sector <input type="checkbox"/> All private sector regardless of size <input type="checkbox"/> All private sector with exceptions depending on size and turnover <input type="checkbox"/> Telecommunications sector <input type="checkbox"/> Health sector (including, for example, private hospitals, day surgeries, medical practitioners, pharmacists, allied health professionals, gyms and weight loss clinics, childcare centres, and medical services in educational institutions) <input type="checkbox"/> Financial Sector (including, for example, banks and credit reporting bodies) <input type="checkbox"/> Other | <p>Year in which mandatory regulation started.</p> <div style="border: 1px solid black; height: 20px; width: 100%;"></div> <div style="border: 1px solid black; height: 20px; width: 100%;"></div> <div style="border: 1px solid black; height: 20px; width: 100%;"></div> <div style="border: 1px solid black; height: 20px; width: 100%;"></div> <div style="border: 1px solid black; height: 20px; width: 100%;"></div> <div style="border: 1px solid black; height: 20px; width: 100%;"></div> <div style="border: 1px solid black; height: 20px; width: 100%;"></div> |
|--|--|

*** If selected Other, please specify:**

If possible, provide URLs of regulatory documents such as the laws, decrees, and guidelines on PDBN reporting:

***QC7. Which of the following aspects trigger the PDBN to data subjects? (Select all that apply)**

- Any breach that poses a risk of harm to or adverse effect on the data subject
- Unauthorised access, regardless of risk of harm to or adverse effect on the data subject
- Unauthorised deletion, regardless of risk of harm to or adverse effect on the data subject
- Unauthorised alteration, regardless of risk of harm to or adverse effect on the data subject
- Unauthorised acquisition, regardless of risk of harm to or adverse effect on the data subject
- Particular types of data, regardless of risk of harm to or adverse effect on the data subject
- Any breach that involves the personal data that is not encrypted
- Scope of breach (such as the number of people impacted)
- Other

*** If selected Other, please specify:**

*** If exceptions or sector-specific requirements apply, please specify:**

***QC8. Within which timeframe is the PDBN to data subjects required? (Select all that apply)**

- Within a prescribed time frame (e.g. 72 hours) where feasible
- Quickly or as soon as possible without unreasonable delay
- Other (please specify)

If exceptions apply or there are several different timeframes, please specify:



[Additional possible question]

***QCx. Is there any requirements on ways to notify personal data breaches to data subjects, such as direct contact via emails or letters, and notification on websites?**

- Yes
- No
- Do not know

***If answered Yes, please specify:**



C-3: DATABASE

***QC9. Does your authority have a database that consolidates all PDBNs reported to your authority (e.g. for internal monitoring, analysis, and investigation purposes)?**

- Yes
- No
- Do not know

*** If answered Yes, please specify what kind of data the PDBN data base contains:**



[Additional possible question]

***QCx. Does your government have a nation-wide database that consolidates all PDBNs reported in your country (e.g. for internal monitoring, analysis, and investigation purposes)?**

- Yes
- No
- Do not know

*** If answered Yes and it is different from what you may specify in QC10, please specify what kind of data the PDBN data base contains:**

D. Personal data breach annual reporting

***QD1. Are statistics on PDBN made publicly available by your authority?**

- Yes, all data are made publicly available
- Yes, but only some data are made publicly available
- No (go to QD2)
- Do not know (go to QD2)

QD1a. Does your authority publish data/statistics on PDBNs at least once a year?

- Yes
- No

QD1b. If possible, please provide an URL or web address for every relevant publicly available source including your data/statistics on PDBNs.

***QD2. Can your authority provide to the OECD the collected data that are relevant to this survey?**

- Yes
- No
- Do not know

E. Number of personal data breach notifications received

***QE1. Are 2020, 2019 and 2018 the most recent reference periods for the record of PDBNs (under voluntary or mandatory arrangements)?**

- Yes
- No

*** If answered No, please specify below your most recent reference periods instead of 2020, 2019 and 2018.**

| | |
|------------------|----------------------|
| Instead of 2020: | <input type="text"/> |
| Instead of 2019: | <input type="text"/> |
| Instead of 2018: | <input type="text"/> |

If the reference periods are not calendar years, please specify.

***QE2. Do you know how many PDBNs (under voluntary or mandatory arrangements) your authority received in 2020, 2019 and 2018 (or reference periods specified above)?**

- Yes
- No (go to next section)

QE2a. If known, please specify the number of PDBNs (under voluntary or mandatory arrangements) your authority received in the reference period.

| | Number of PDBNs |
|---|----------------------|
| In 2020 (or reference period specified above) | <input type="text"/> |
| In 2019 (or reference period specified above) | <input type="text"/> |
| In 2018 (or reference period specified above) | <input type="text"/> |

QE2b. If known, please specify the number of PDBNs (under voluntary or mandatory arrangements) your authority received in the reference period and that is notified to the data subjects as well.

| | Number of PDBNs |
|---|----------------------|
| In 2020 (or reference period specified above) | <input type="text"/> |
| In 2019 (or reference period specified above) | <input type="text"/> |
| In 2018 (or reference period specified above) | <input type="text"/> |

[Additional possible question]

QEx. Does your authority record the following figures related to reported personal data breaches? (Select all that apply)

| | |
|--------------------------|---|
| <input type="checkbox"/> | Number of the affected data subjects within your authority's jurisdiction |
| <input type="checkbox"/> | Number of all the affected data subjects beyond your authority's jurisdiction |
| <input type="checkbox"/> | Size of breached data |

F. Personal data breach notification by sector

***QF1. Are PDBNs recorded by the sector in which the breaches occur?**

- Yes
- No (go to next section)
- Do not know (go to next section)

***QF2. Are 2020, 2019 and 2018 your most recent reference periods for PDBN record by sector?**

- Yes
- No

*** If answered No, please specify below your most recent reference periods instead of 2020, 2019, and 2018:**

| | |
|------------------|----------------------|
| Instead of 2020: | <input type="text"/> |
| Instead of 2019: | <input type="text"/> |

Instead of 2018:

***QF3. Which industry classification is used to report on PDBNs by sector?**

- International Standard Industrial Classification of All Economic Activities (ISIC Rev.4)
- National industry classification
- Do not know
- Other

*** If selected National industry classification or Other, please specify. If possible, provide URLs of documents that show correspondence to international industrial classification:**

QF4. Please provide, where available, the number of PDBNs by sector.

| | In 2020 (or reference period specified above) | In 2019 (or reference period specified above) | In 2018 (or reference period specified above) |
|--|---|--|---|
| Agriculture, forestry and fishing | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Manufacturing | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Energy (e.g. electricity, gas, steam, air conditioning supply), water supply, sewerage, waste management and remediation activities) | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Construction | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Wholesale and retail trade | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Transportation and storage | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Accommodation (e.g. hotels) and food service activities | <input type="text"/> | <input type="text"/> | <input type="text"/> |

| | | | |
|---|----------------------|----------------------|----------------------|
| Information and communication (e.g. publishing, telecommunications) | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Financial and insurance activities | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Real estate activities | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Professional, scientific, technical, administrative and support service activities (e.g. legal and accounting activities, scientific research and development, advertising and market research) | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Public administration and defence; compulsory social security | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Education | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Human health and social work activities | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Other service activities | <input type="text"/> | <input type="text"/> | <input type="text"/> |

* If selected Other service activities, please specify:

G. The nature and type of the personal data breach incident

***QG1. Does your authority collect information on the nature and the type of personal data breach?**

- Yes
- No (go to QG4)
- Do not know (go to QG4)

***QG2. Is it possible to classify the PDBN data that are collected into availability breach, integrity breach, and confidentiality breach, where a breach can be one or more types?**

Please see the glossary for definition of breaches

- Yes
 No
 Do not know

*** If answered No, please explain why:**

***QG3. Is it possible to classify the PDBN data that are collected by the following nature of causes of the event?**

| | Yes | No | Do Not Know |
|-----------------------------------|-----------------------|-----------------------|-----------------------|
| Malicious or non-malicious | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Internal or external | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Human error | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

[Additional possible alternatives]
“Non-digital processes” and “Cross-border”

*** If answered No, please specify why for each:**

[Additional possible question]

***QGx. Does your authority collect information on near misses of personal data breach?**

- Yes
 No (go to QG8)
 Do not know (go to QG8)

*** If answered Yes, please specify:**

***QG4. Is it possible to classify the PDBN data that are collected into the following sub-categories?**

| | Yes | No | Do not know |
|--|-----------------------|-----------------------|----------------------------------|
| Loss of IT equipment – misplaced or stolen equipment – laptops, USB sticks etc. | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| Mailing – distribution of a letter in the mail or an email to an incorrect address that includes personal data | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Hacking – malicious attacks on computer networks | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Theft – data in the form of documents, electronically stored data, etc. that is stolen | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Unauthorised access – employees taking advantage of vulnerabilities to access personal data of customers stored in files or electronically | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Other | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

*** If selected Other, please specify:**

[Additional possible alternatives]
“Improper disposal of documents”, “Technical error”, and “Unauthorised disclosure”

H. The types of personal data affected

***QH1. Does your authority collect information on the types of personal data breached?**

- Yes, for all the reported PDBNs
- Yes, but only for a subset of PDBN cases
- No (go to QH3)

Do not know (go to QH3)

*** If selected the second alternative, please specify for what kinds of cases your authority collect information on the types of personal data breached:**

***QH2. Is it possible to classify the data into the following sub-categories?**

| | Yes | No | Do not know |
|--|-----------------------|-----------------------|-----------------------|
| Personal credential data (e.g. national identification number or official document, contact details, full name, data on education, family life, professional experience) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Sensitive data (e.g. personal health data, political affiliation, sex life) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Financial data (e.g. income, financial transactions, bank statements, investments, credit cards, invoices) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Other | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

*** If selected Other, please specify:**

[Additional possible alternatives]
“Behavioural data (e.g., location, traffic data, data on personal preferences and habits)”

***QH3. Does your authority collect information on whether the personal data were encrypted?**

- Yes, for all the reported PDBNs
- Yes, but only for a subset of PDBN cases
- No
- Do not know

*** If selected the second alternative, please specify for what kinds of cases your authority collect information on the types of personal data breached:**

I. Monetary fines and other penalties

***QI1. Are fines administered for personal data breaches in your jurisdiction?**

- Yes
- No (go to QI4)
- Do not know (go to QI4)

[Additional possible question]

***QIx. Is the most recent reference period 2020 for the record of fines administered?**

- Yes
- No

*** If answered No, please specify below your most recent reference period instead of 2020.**

Instead of 2020:

QIxa. Please provide the total amount and currency of fines administered for personal data breaches:

Amount Currency

***QI2. Is your authority responsible for administering fines?**

- Yes
- No
- Do not know

*** If answered No, please specify.**

QI3. Is your authority aware of significant private enforcement of data breaches by individuals or those collectively representing individuals? If so, what sanctions or remedies have been imposed? If possible, please provide links to relevant documents.

QI4. Is your authority aware of enforcement activities by other authorities not represented in this survey? If possible, please provide links to relevant documents.

***QI5. Are there any other regulatory actions taken in response to a PDBN (or lack of breach notification), which would include imposing other requirements upon the reporting organisation?**

- Yes
- No
- Do not know

*** If answered Yes, please specify:**

***QI6. Has your authority initiated audits/investigations in response to the following?**

| | Yes | No | Do not know |
|---|-----------------------|-----------------------|-----------------------|
| Reported PDBNs by data controllers | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Information from influenced data subjects | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Information from other public authorities (e.g. responsible for digital security, consumer policy, law enforcement, etc.) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Information related to personal data breach on the media | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Other | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

*** If selected Other, please specify:**

[Additional possible alternatives]

“Information from other private and public bodies”, “Detection of personal data breaches by your authority”, and “Information about personal data breaches shared from non-affected individuals”

J. Measures taken to prevent or mitigate risk and impact evaluation

***QJ1. Does your authority verify the authenticity of reported PDBNs?**

- Yes, for all the reported PDBNs
- Yes, but only for a subset of PDBN cases (e.g. when most impactful)
- No
- Do not know

*** If answered Yes, please specify:**

***QJ2. Does your authority check what organisational and technical measures the breached organisation had taken before the reported PDB happened?**

- Yes, for all the reported PDBNs
- Yes, but only for a subset of PDBN cases (e.g. when most impactful)
- No
- Do not know

*** If answered Yes, please specify under what condition your authority does so:**

[Additional possible questions]

***QJx. Does your authority investigate the economic and social impacts on the organisation that reported a PDBN?**

- Yes, for all the reported PDBNs
- Yes, but only for a subset of PDBN cases (e.g. when most impactful)
- No
- Do not know

*** If answered Yes, does your authority examine the following impact types:**

| | Yes | No | Do not know |
|--|-----------------------|-----------------------|-----------------------|
| Technical investigation and recovery activity (e.g. digital forensic and IT system replacement) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Improvement of digital security (e.g. establishment of cross-departmental CSIRT, introduction of technical measure to detect incidents, employee training) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Fines and fulfilment of regulatory requirements | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Other | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

[Additional possible alternatives]

“Loss of monetary value that otherwise breached personal data would create”, “Private litigation with stakeholders”, “Disrupted operation”, “Public relation”, “Activity to keep current customers”, “Loss of revenues”, “Loss of customer base”, “Change in stock price”, and “Increase in insurance premium and debt raising”

K. Use of PDBN data

***QK1. Does your authority use the PDBN data for resource and strategic planning for the next year and improving operation within the authority?**

- Yes
- No
- Do not know

*** If answered Yes, please specify:**

***QK2. Does your authority use the PDBN data for improving public relations to raise awareness of targeted sectors and entities such as SMEs as well as awareness about certain risks?**

- Yes
- No
- Do not know

*** If answered Yes, please specify:**

***QK3. Does your authority use the PDBN data for improving guidance and guidelines that are issued by your authority on the following measures that the data controller is required or recommended to implement?**

| | Yes | No | Do not know |
|--|-----------------------|-----------------------|-----------------------|
| Organisational measures (e.g. establishment of Chief Data Officer, reporting procedure of data breach, plan–do–check–adjust (PDCA) cycle of risk management, employee education, etc.) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Technical measures on digital processes (e.g. encryption, access control, protective measures for external threats, log monitoring, vulnerability management, etc.) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Technical measures on physical environment (e.g. control of the area where to deal with personal data, measures against theft and lost, disposal of medium and devices, etc.) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Other | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

*** If selected Other, please specify:**

***QK4. Does your authority use the PDBN data for reinforcing the collaboration with other authorities responsible for digital security, consumer policy, law enforcement, etc.?**

- Yes
- No
- Do not know

* If answered Yes, please specify:

[Additional possible question]

*QKx. Does your authority use the PDBN data for evaluating the economic impacts of PDB within your authority's jurisdiction or geographical scope?

- Yes
 No
 Do not know

* If answered Yes, please specify:

Glossary of Terms

Personal Data Breach (PDB): Although definitions vary, a ‘personal data breach’ can be described broadly as being a breach of security that leads to the unintended or unauthorised destruction, loss, alteration, disclosure of, or access to personal data. It is important to distinguish this from the more general term ‘data breach’ which can be used to refer to security incidents that impact on non-personal data as well as on personal data. Personal data breaches are a sub set of data breaches.

Personal Data Breach Notification (PDBN): There is a growing body of legal and regulatory requirements that govern disclosures or notifications that (public and private) organisations are required or encouraged to make following a personal data breach. These may be disclosures to a privacy enforcement authority (PEA) where one exists or to other regulators such as those with responsibility for the oversight of financial services or telecommunications. There may also be disclosures to affected individuals whose personal data has been compromised by the breach.

Full-Time Equivalent (FTE): According to OECD and Eurostat, a full-time equivalent is a unit to measure employed persons in a way that makes them comparable although they may work a different number of hours per week. The unit is obtained by comparing an employee's average number of hours worked to the average number of hours of a full-time worker. A full-time person is therefore counted as one FTE, while a part-time worker gets a score in proportion to the hours he or she works. For example, a part-time worker employed for 20 hours a week where full-time work consists of 40 hours, is counted as 0.5 FTE. The workforce of an enterprise, activity, or country etc. can then be added up and expressed as the number of full-time equivalents.

International Standard Industrial Classification of All Economic Activities (ISIC): The international reference classification of productive activities. Its main purpose is to provide a set of activity categories that can be utilised for the collection and reporting of statistics according to such activities. Please refer to page 42 on https://unstats.un.org/unsd/publication/SeriesM/seriesm_4rev3_1e.pdf

Proposed High Level Breach Classification:

- Availability Breach– where there is an accidental or unauthorised loss of access to, or destruction of, personal data
- Integrity Breach– where there is an unauthorised or accidental alteration of personal data.
- Confidentiality Breach– where there is an unauthorised or accidental disclosure of, or access to, personal data

Proposed Classification of Personal Data Breach Types:

- Personal credential data– e.g. national identification number or official document, contact details, full name, data on education, family life, professional experience
- Sensitive data– e.g. personal health data, political affiliation, sex life
- Financial data– e.g. Income, financial transactions, bank statements, investments, credit cards, invoices
- Behavioural data– e.g. geolocation data, traffic data, data on personal preferences and habits

ANNEX B. Survey questionnaire administered from June 2019 to February 2020

A. General questions and authority profile

QA1. Please provide the name and contact email address of the person completing this survey:

These details will not be released but will enable the OECD Secretariat to clarify responses if necessary.

| | Name | E-mail address |
|------------------|----------------------|----------------------|
| Contact details: | <input type="text"/> | <input type="text"/> |

***QA2. Please provide the name of your Privacy Enforcement Authority (PEA):**

***QA2a. Please select your country:**

***QA3. What is the jurisdiction or geographical scope of the authority?**

- Federal/National
- Local/Provincial/State/Regional
- International/Supranational

***QA4. Is your authority involved in enforcing regulation on personal data breach notification (PDBN)?**

- Yes
- No
- Do not know

***QA5. Does your authority oversee privacy protection practices by the following sectors? (Select all that apply)**

- the public sector

- the private sector
- the non-profit sector (NPOs, charities, etc.)

***QA6. In addition to roles under a data protection or privacy law mandate and power, does your authority perform other regulatory or oversight functions? (e.g. under the Government information access or Freedom of Information law)**

- Yes
- No
- Do not know

***If answered Yes, please specify what other regulatory or oversight functions are performed:**

B. Authority’s funding and human resources

Please note: If there are more than one PEAs in your country, report information only for your own authority. If your authority is funded over a longer period than one year (e.g. 2 or 5 years), please report for all of the questions in this section funding estimates broken down by year. If your authority does not use calendar year, please specify the relevant reference periods (e.g. fiscal year) as indicated in the questions below.

FUNDING

***QB1. Are 2019, 2018 and 2017 your most recent reference periods for providing funding information?**

- Yes
- No

Any additional comments:

*** If answered No, please specify below your most recent reference periods for funding information, instead of 2018 and 2017.**

| | |
|------------------|----------------------|
| Instead of 2019: | <input type="text"/> |
| Instead of 2018: | <input type="text"/> |
| Instead of 2017: | <input type="text"/> |

***QB2. Do you know what the total budget of your authority was in 2019 (or most recent reference period)?**

- Yes
- No (go to QB4)

Any additional comments:

QB2a. If known, please specify the total budget including all sources of funding (e.g. government grants, registration or licensing fees, chargeable services and fines and penalties).

| | Amount | Currency |
|---|----------------------|--|
| In 2019 (or reference period specified above) | <input type="text"/> | Select: <input type="text" value="▼"/> |
| In 2018 (or reference period specified above) | <input type="text"/> | Select: <input type="text" value="▼"/> |
| In 2017 (or reference period specified above) | <input type="text"/> | Select: <input type="text" value="▼"/> |

***QB3. Does your authority’s funding in 2019 (or most recent reference period) which was answered in QB2a originate from any of the following sources?**

| | Yes | No | Do not know | If YES, percentage of total funding if known |
|---|-----------------------|-----------------------|-----------------------|--|
| Government funding | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="text"/> |
| Registration or licensing fees | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="text"/> |
| Chargeable services (e.g. auditing, training, publications) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="text"/> |
| Fines and penalties | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="text"/> |
| Other | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="text"/> |

*** If selected Other, please specify:**

HUMAN RESOURCES

***QB4. Are 2019, 2018 and 2017 your most recent reference periods for resource information (on the number of staff)?**

- Yes
- No

*** If answered No, please specify below your most recent reference periods for resource information (on the number of staff), instead of 2019, 2018 and 2017.**

| | |
|------------------|--|
| Instead of 2019: | |
| Instead of 2018 | |
| Instead of 2017: | |

*** QB5. Do you know how much staff is employed by your authority (full time equivalent employees)?**

- Yes
- No (go to next section)

QB5a. If known, please specify the total number of staff employed (full time equivalent employees).

| | Number of staff |
|---|---|
| In 2019 (or reference period specified above) | <input style="width: 100%;" type="text"/> |
| In 2018 (or reference period specified above) | <input style="width: 100%;" type="text"/> |
| In 2017 (or reference period specified above) | <input style="width: 100%;" type="text"/> |

QB5b. If known, please specify the number of staff employed (full time equivalent employees) in the department/division/section that deals with PDBN.

| | Number of staff |
|---|---|
| In 2019 (or reference period specified above) | <input style="width: 100%;" type="text"/> |
| In 2018 (or reference period specified above) | <input style="width: 100%;" type="text"/> |
| In 2017 (or reference period specified above) | <input style="width: 100%;" type="text"/> |

C. Personal data breach notification reporting law, jurisdiction and exemptions

***QC1. Is there a mandatory requirement to report personal data breaches to one or more enforcement authorities in your jurisdiction?**

- Yes (go to QC2)
- No (go to QC1a)
- Do not know (go to QC2)

*** If answered Yes, please specify the enforcement authority/authorities:**

***QC1a. Will PDBNs become mandatory in the next two years?**

- Yes, a new law or other policy requirement has been passed and will come into force within the next two years (go to QC6)
- Probably, a new law or other policy requirement is expected to be in force within the next two years (go to QC6)
- No (go to QC6)
- Do not know (go to QC6)

***QC2. Does the mandatory PDBN reporting to the enforcement authority/authorities apply generally or to particular sectors? (Select all that apply)**

| | Year in which mandatory regulation started. |
|---|--|
| <input type="checkbox"/> Generally | <input style="width: 100px; height: 20px;" type="text"/> |
| <input type="checkbox"/> All public sector | <input style="width: 100px; height: 20px;" type="text"/> |
| <input type="checkbox"/> All private sector regardless of size | <input style="width: 100px; height: 20px;" type="text"/> |
| <input type="checkbox"/> All private sector with exceptions depending on size and turnover | <input style="width: 100px; height: 20px;" type="text"/> |
| <input type="checkbox"/> Telecommunications sector | <input style="width: 100px; height: 20px;" type="text"/> |
| <input type="checkbox"/> Health sector (including, for example, private hospitals, day surgeries, medical practitioners, pharmacists, allied health professionals, gyms and weight loss clinics, childcare centres, and medical services in educational institutions) | <input style="width: 100px; height: 20px;" type="text"/> |
| <input type="checkbox"/> Financial Sector (including, for example, banks and credit reporting bodies) | <input style="width: 100px; height: 20px;" type="text"/> |
| <input type="checkbox"/> Other | <input style="width: 100px; height: 20px;" type="text"/> |

*** If selected Other, please specify:**

If possible, provide URLs of regulatory documents such as the laws, decrees, and guidelines on PDBN:

***QC3. Which of the following aspects trigger the PDBN to the enforcement authority/authorities? (Select all that apply)**

- Any breach that poses a risk of harm to or adverse effect on the data subject
- Unauthorised access, regardless of risk of harm to or adverse effect on the data subject
- Unauthorised deletion, regardless of risk of harm to or adverse effect on the data subject
- Unauthorised alteration, regardless of risk of harm to or adverse effect on the data subject
- Unauthorised acquisition, regardless of risk of harm to or adverse effect on the data subject
- Particular types of data, regardless of risk of harm to or adverse effect on the data subject
- Scope of breach (such as the number of people impacted)
- Other

*** If selected Other, please specify:**

*** If exceptions or sector-specific requirements apply, please specify:**

***QC4. Within which timeframe is the PDBN to the enforcement authority/authorities required? (Select all that apply)**

- Within a prescribed time frame (e.g. 72 hours) where feasible
- Quickly or as soon as possible without unreasonable delay
- Other (please specify)

If exceptions apply or there are several different timeframes, please specify:

***QC5. Does the mandatory PDBN reported above also include specific requirements for data subject notification?**

- Yes
- No (go to QC6)
- Do not know (go to QC6)

*** If answered Yes, are the requirements to notify the data subject in terms of trigger and timeframe different to those specified above in QC3 and QC4?**

- Yes
- No
- Do not know

*** If answered Yes, please explain further (e.g. when data subjects need to be notified):**

***QC5a. Do the requirements in QC5 provide guidance on how and when to notify individuals in other jurisdictions?**

- Yes
- No
- Do not know

***If answered Yes, please specify:**

***QC6. Has a central database that consolidates all PDBNs reported in your country (e.g. for internal monitoring, analysis, and investigation purposes)?**

- Yes
- No
- Do not know

*** If answered Yes, please specify what kind of data the PDBN data base contains:**

***QC7. Please describe if and under what circumstances the relevant authority expects voluntary personal data breach reporting:**

D. Personal data breach annual reporting

***QD1. Are statistics on PDBN made publicly available by your authority?**

- Yes, all data are made publicly available
- Yes, but only some data are made publicly available
- No (go to QD2)
- Do not know (go to QD2)

QD1a. Does your authority publish data/statistics on PDBNs at least once a year?

- Yes
- No

QD1b. If possible, please provide an URL or web address for every relevant publicly available source including your data/statistics on PDBNs.

***QD2. Can your authority provide to the OECD the collected data that are relevant to this survey?**

- Yes
- No
- Do not know

E. Number of personal data breach notifications received

***QE1. Are 2019, 2018 and 2017 the most recent reference periods for the record of PDBNs (under voluntary or mandatory arrangements)?**

- Yes
- No

*** If answered No, please specify below your most recent reference periods instead of 2019, 2018 and 2017.**

| | |
|------------------|----------------------|
| Instead of 2019: | <input type="text"/> |
| Instead of 2018: | <input type="text"/> |
| Instead of 2017: | <input type="text"/> |

***QE2. Do you know how many PDBNs (under voluntary or mandatory arrangements) your authority received in 2019, 2018 and 2017 (or reference periods specified above)?**

- Yes
- No (go to next section)

QE2a. If known, please specify the number of PDBNs (under voluntary or mandatory arrangements) your authority received in the reference period.

| | Number of PDBNs |
|--|----------------------|
| In 2019 (or reference period specified above) | <input type="text"/> |
| In 2018 (or reference period specified above) | <input type="text"/> |
| In 2017 (or reference period specified above) | <input type="text"/> |

QE2b. If known, please specify the number of PDBNs (under voluntary or mandatory arrangements) your authority received in the reference period and that is notified to the data subjects as well.

| | Number of PDBNs |
|--|----------------------|
| In 2019 (or reference period specified above) | <input type="text"/> |
| In 2018 (or reference period specified above) | <input type="text"/> |
| In 2017 (or reference period specified above) | <input type="text"/> |

***QE3. Does your authority record the total number of individuals that were affected in 2019, 2018, and 2017 in your country (or reference period specified above)?**

- Yes
- No (go to next section)
- Do not know (go to next section)

If answered Yes, please specify the total number of individuals:

| | Number of individuals |
|--|-----------------------|
| In 2019 (or reference period specified above) | <input type="text"/> |
| In 2018 (or reference period specified above) | <input type="text"/> |
| In 2017 (or reference period specified above) | <input type="text"/> |

F. Personal data breach notification by sector

***QF1. Are PDBNs recorded by the sector in which the breaches occur?**

- Yes
- No (go to next section)
- Do not know (go to next section)

***QF2. Are 2019, 2018 and 2017 your most recent reference periods for PDBN record by sector?**

- Yes
- No

*** If answered No, please specify below your most recent reference periods instead of 2017 and 2016:**

| | |
|------------------|----------------------|
| Instead of 2019: | <input type="text"/> |
| Instead of 2018: | <input type="text"/> |
| Instead of 2017: | <input type="text"/> |

***QF3. Which industry classification is used to report on PDBNs by sector?**

- International Standard Industrial Classification of All Economic Activities (ISIC Rev.4)
- National industry classification
- Do not know
- Other

* If selected Other, please specify:

QF4. Please provide, where available, the number of PDBNs by sector.

| | In 2019 (or reference period specified above) | In 2018 (or reference period specified above) | In 2017 (or reference period specified above) |
|--|---|--|---|
| Agriculture, forestry and fishing | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Manufacturing | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Energy (e.g. electricity, gas, steam, air conditioning supply), water supply, sewerage, waste management and remediation activities) | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Construction | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Wholesale and retail trade | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Transportation and storage | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Accommodation (e.g. hotels) and food service activities | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Information and communication (e.g. publishing, telecommunications) | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Financial and insurance activities | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Real estate activities | <input type="text"/> | <input type="text"/> | <input type="text"/> |

| | | | |
|---|----------------------|----------------------|----------------------|
| Professional, scientific, technical, administrative and support service activities (e.g. legal and accounting activities, scientific research and development, advertising and market research) | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Public administration and defence; compulsory social security | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Education | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Human health and social work activities | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| Other service activities | <input type="text"/> | <input type="text"/> | <input type="text"/> |

* If selected Other, please specify:

G. The nature and type of the personal data breach incident

***QG1. Does your authority collect information on the nature and the type of personal data breach?**

- Yes
- No (go to QG4)
- Do not know (go to QG4)

***QG2. Is it possible to classify the PDBN data that are collected into availability breach, integrity breach, and confidentiality breach, where a breach can be one or more types?**

Please see the glossary for definition of breaches (see Annex A)

- Yes
- No
- Do not know

*** If answered No, please explain why:**

***QG3. Is it possible to classify the PDBN data that are collected by the following nature of causes of the event?**

| | Yes | No | Do Not Know |
|-----------------------------------|-----------------------|-----------------------|-----------------------|
| Malicious or non-malicious | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Internal or external | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Human error | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Non-digital processes | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Cross-border | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

*** If answered No, please specify why for each:**

***QG4. Does your authority collect information on near misses of personal data breach?**

- Yes
- No (go to QG8)
- Do not know (go to QG8)

*** If answered Yes, please specify:**

QG5. Are the near misses voluntarily reported?

- Yes
- No
- Do not know

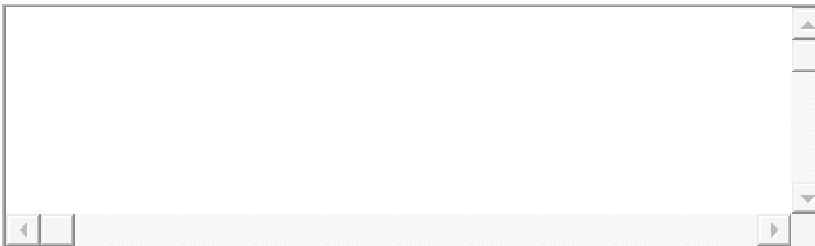
*** If answered Yes, please specify:**

A large, empty rectangular text box with a light gray background and a thin border. It has a vertical scrollbar on the right side and horizontal scrollbars at the bottom, indicating it is a scrollable area for text input.

QG6. Does the near miss reporting depend on sector?

- Yes
- No
- Do not know

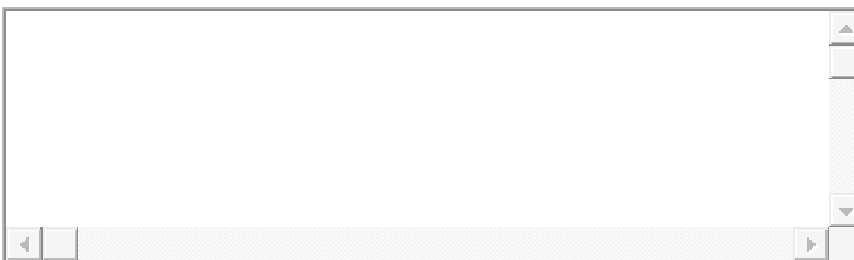
*** If answered Yes, please specify:**

A large, empty rectangular text box with a light gray background and a thin border. It has a vertical scrollbar on the right side and horizontal scrollbars at the bottom, indicating it is a scrollable area for text input.

QG7. Is there any benefit for reporters of near misses?

- Yes
- No
- Do not know

*** If answered Yes, please specify:**

A large, empty rectangular text box with a light gray background and a thin border. It has a vertical scrollbar on the right side and horizontal scrollbars at the bottom, indicating it is a scrollable area for text input.

***QG8. Is it possible to classify the PDBN data that are collected into the following sub-categories?**

| | Yes | No | Do not know |
|--|-----------------------|-----------------------|----------------------------------|
| Loss of IT equipment – misplaced or stolen equipment – laptops, USB sticks etc. | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| Mailing – distribution of a letter in the mail or an email to an incorrect address that includes personal data | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Improper disposal of documents – leaving personal data in documents deposited in a garbage bin that can be accessed by the public | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Hacking – malicious attacks on computer networks | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Technical error – unforeseen complication in an IT system exposing data to outside parties | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Theft – data in the form of documents, electronically stored data, etc. that is stolen | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Unauthorised access – employees taking advantage of vulnerabilities to access personal data of customers stored in files or electronically | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Unauthorised disclosure– e.g. distributing personal data on P2P networks | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Other | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

*** If selected Other, please specify:**

H. The types of personal data affected

***QH1. Does your authority collect information on the types of personal data breached?**

- Yes, for all the reported PDBNs
- Yes, but only for a subset of PDBN cases
- No (go to QH3)
- Do not know (go to QH3)

*** If selected the second alternative, please specify for what kinds of cases your authority collect information on the types of personal data breached:**

***QH2. Is it possible to classify the data into the following sub-categories?**

| | Yes | No | Do not know |
|--|-----------------------|-----------------------|-----------------------|
| Personal credential data (e.g. national identification number or official document, contact details, full name, data on education, family life, professional experience) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Sensitive data (e.g. personal health data, political affiliation, sex life) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Behavioural data (e.g., location, traffic data, data on personal preferences and habits) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Financial data (e.g. income, financial transactions, bank statements, investments, credit cards, invoices) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Other | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

*** If selected Other, please specify:**

***QH3. Does your authority collect information on whether the personal data were encrypted?**

- Yes, for all the reported PDBNs
- Yes, but only for a subset of PDBN cases
- No
- Do not know

*** If selected the second alternative, please specify for what kinds of cases your authority collect information on the types of personal data breached:**

I. Monetary fines and other penalties

***QI1. Are fines administered for personal data breaches in your jurisdiction?**

- Yes
- No (go to QI4)
- Do not know (go to QI4)

***QI2. Is the most recent reference period 2019 for the record of fines administered?**

- Yes
- No

*** If answered No, please specify below your most recent reference period instead of 2019.**

Instead of 2019:

QI2a. Please provide the total amount and currency of fines administered for personal data breaches:

Amount Currency

***QI3. Is your authority responsible for administering fines?**

- Yes
- No
- Do not know

*** If answered No, please specify.**

***QI4. Are there any other regulatory actions taken in response to a PDBN (or lack of breach notification), which would include imposing other requirements upon the reporting organisation?**

- Yes
- No
- Do not know

*** If answered Yes, please specify:**

***QI5. Has your authority initiated audits/investigations in response to the following?**

| | Yes | No | Do not know |
|---|-----------------------|-----------------------|-----------------------|
| Reported PDBNs by data controllers | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Information from influenced data subjects | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Information from other public authorities (e.g. responsible for digital security, consumer policy, law enforcement, etc.) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Information from other private and public bodies (e.g. cybersecurity firms, CSIRTs, NPOs, etc.) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Information related to personal data breach on the media | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Detection of PDBN by your authority | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Information about personal data breach shared from non-affected individuals | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Other | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

*** If selected Other, please specify:**

J. Measures taken to prevent or mitigate risk and impact evaluation

***QJ1. Does your authority verify the authenticity of reported PDBNs?**

- Yes, for all the reported PDBNs
- Yes, but only for a subset of PDBN cases (e.g. when most impactful)
- No
- Do not know

*** If answered Yes, please specify:**

***QJ2. Does your authority check what organisational and technical measures the breached organisation had taken before the reported PDB happened?**

- Yes, for all the reported PDBNs
- Yes, but only for a subset of PDBN cases (e.g. when most impactful)
- No
- Do not know

*** If answered Yes, please specify under what condition your authority does so:**

***QJ3. Does your authority investigate the economic and social impacts on the organisation that reported a PDBN?**

- Yes, for all the reported PDBNs
- Yes, but only for a subset of PDBN cases (e.g. when most impactful)
- No
- Do not know

*** If answered Yes, does your authority examine the following impact types:**

| | Yes | No | Do not know |
|---|-----------------------|-----------------------|-----------------------|
| Technical investigation and recovery activity (e.g. digital forensic and IT system replacement) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

| | | | |
|--|-----------------------|-----------------------|-----------------------|
| Improvement of digital security (e.g. establishment of cross-departmental CSIRT, introduction of technical measure to detect incidents, employee training) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Loss of monetary value that otherwise breached personal data would create in the future | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Private litigation with stakeholders | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Fines and fulfilment of regulatory requirements | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Disrupted operation (e.g. additional staff working to deal with PDB, period of stopped production) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Public relation (conduct of press releases and other outreach activities) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Activity to keep current customers (discounts offered to those affected, loyalty program) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Loss of revenue | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Loss of customer base | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Change in stock price | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Increase in insurance premium and debt raising | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Other | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

K. Use of PDBN data

***QK1. Does your authority use the PDBN data for budget planning for the next year and improving operation within the authority?**

- Yes
- No
- Do not know

*** If answered Yes, please specify:**

***QK2. Does your authority use the PDBN data for improving public relations to raise awareness of targeted sectors and entities such as SMEs as well as awareness about certain risks?**

- Yes
- No
- Do not know

*** If answered Yes, please specify:**

***QK3. Does your authority use the PDBN data for improving the guideline on the following measures that the data controller is required to implement?**

| | Yes | No | Do not know |
|--|-----------------------|-----------------------|-----------------------|
| Organisational measures (e.g. establishment of Chief Data Officer, reporting procedure of data breach, plan–do–check–adjust (PDCA) cycle of risk management, employee education, etc.) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Technical measures on digital processes (e.g. encryption, access control, protective measures for external threats, log monitoring, vulnerability management, etc.) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Technical measures on physical environment (e.g. control of the area where to deal with personal data, measures against theft and lost, disposal of medium and devices, etc.) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Other | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

*** If selected Other, please specify:**

***QK4. Does your authority use the PDBN data for reinforcing the collaboration with other authorities responsible for digital security, consumer policy, law enforcement, etc.?**

- Yes
- No
- Do not know

*** If answered Yes, please specify:**

***QK5. Does your authority use the PDBN data for evaluating the economic impacts of PDB within your authority’s jurisdiction or geographical scope?**

- Yes
- No
- Do not know

*** If answered Yes, please specify:**

Glossary of Terms

Personal Data Breach (PDB): Although definitions vary, a ‘personal data breach’ can be described broadly as being a breach of security that leads to the unintended or unauthorised destruction, loss, alteration, disclosure of, or access to personal data. It is important to distinguish this from the more general term ‘data breach’ which can be used to refer to security incidents that impact on non-personal data as well as on personal data. Personal data breaches are a sub set of data breaches.

Personal Data Breach Notification (PDBN): There is a growing body of legal and regulatory requirements that govern disclosures or notifications that (public and private) organisations are required or encouraged to make following a personal data breach. These may be disclosures to a privacy enforcement authority (PEA) where one exists or to other regulators such as those with responsibility for the oversight of financial services or telecommunications. There may also be disclosures to affected individuals whose personal data has been compromised by the breach.

Full-Time Equivalent (FTE): According to OECD and Eurostat, a full-time equivalent is a unit to measure employed persons in a way that makes them comparable although they may work a different number of hours per week. The unit is obtained by comparing an employee’s average number of hours worked to the average number of hours of a full-time worker. A full-time person is therefore counted as one FTE, while a part-time worker gets a score in proportion to the hours he or she works. For example, a part-time worker employed for 20 hours a week where full-time work consists of 40 hours, is counted as 0.5 FTE. The workforce of an enterprise, activity, or country etc. can then be added up and expressed as the number of full-time equivalents.

International Standard Industrial Classification of All Economic Activities (ISIC): The international reference classification of productive activities. Its main purpose is to provide a set of activity categories that can be utilised for the collection and reporting of statistics according to such activities. Please refer to page 42 on https://unstats.un.org/unsd/publication/SeriesM/seriesm_4rev3_1e.pdf

Proposed High Level Breach Classification:

- Availability Breach– where there is an accidental or unauthorised loss of access to, or destruction of, personal data

- Integrity Breach– where there is an unauthorised or accidental alteration of personal data.
- Confidentiality Breach– where there is an unauthorised or accidental disclosure of, or access to, personal data

Proposed Classification of Personal Data Breach Types:

- Personal credential data– e.g. national identification number or official document, contact details, full name, data on education, family life, professional experience
- Sensitive data– e.g. personal health data, political affiliation, sex life
- Financial data– e.g. Income, financial transactions, bank statements, investments, credit cards, invoices
- Behavioural data– e.g. geolocation data, traffic data, data on personal preferences and habits

Notes

¹In addition to state and territorial breach notification laws, several laws require breach notification at the US federal level. The Health Insurance Portability and Accountability Act (HIPAA) requires HIPAA-covered entities and their business associates to provide notification following a breach of unsecured protected health information. The Health Information Technology for Economic and Clinical Health (HITECH) Act requires breach notification as to personal health records. Certain federal regulators also enforce breach notification obligations that apply to financial institutions under the Gramm-Leach-Bliley Safeguards Rule.

² European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*, O.J. (L 119) 32 (General Data Protection Regulation).

³ National Conference of State Legislature provides citations to each state's data breach notification law [here](#).

⁴ Carter, 2009, 'A 50-State Report on Unfair and Deceptive Act and Practices Statutes', available [here](#). National Freedom of Information Coalition, n.d., 'State Freedom of Information Laws', available [here](#).

⁵ There are potential drawbacks with this approach such as overrepresentation of changes when the real initial value is smaller (in particular, zero) or underrepresentation when higher. However, this data representation is useful to uncover trends.

⁶ California SB 1386, 2002, available [here](#).

⁷ In Canada, the results reported for the private sector are only for those organisations subject to federal law (the Personal Information Protection and Electronic Documents Act). As such, the results would not include data breaches that are required to be reported under provincial or territorial private-sector privacy law.

⁸ Exceptions to the reporting obligations under the Notifiable Data Breach scheme exist in relation to enforcement related activities, where other legal requirements exist, where the Privacy Enforcement Authority has declared that an organisation or agency does not need to comply, or sometimes where a data breach involves more than one entity.

⁹ Wash. Rev. Code §§ 19.255.010 (1).

¹⁰ Article 4(12) provides that: “Personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.”

¹¹ Article 33(1) provides that: “In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.”

¹² Article 2(h) provides that: “Personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.”

¹³ Article 4(3) provides that: “In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority.”

¹⁴ Article 12(5) provides that: “In case the data processed are obtained by others by unlawful means, the data controller shall communicate the breach to the data subject and notify it to the Board within the shortest time. Where necessary, the Board may announce such breach at its official website or through in any other way it deems appropriate.”

¹⁵ Article 38 provides that: “In addition to those specified in the relevant laws and in applicable regulations, any of the following events, listed here as a minimum, are considered to be security breaches at any phase in the processing of personal data: loss or unauthorized destruction; theft, misplacement or unauthorized copying; unauthorized use, access or processing; and damage to and unauthorized alteration or modification.”

¹⁶ Article 40 provides that: “The data controller must forthwith inform the data owner and, as applicable, the Institute and the Guarantor bodies of the Federated States, on any breaches that significantly affect economic or moral rights, upon confirmation that a breach has occurred, and once the data controller has begun to take the action required to trigger in-depth examination in regard to the extent of the breach, so as to enable affected data owners to take the required measures to defend their rights.”

¹⁷ To be precise, unauthorised use is included in Canada thresholds, as Principle 7 in the Personal Information Protection and Electronic Documents Act notes: “The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.” In addition, for government institution reporting, a privacy breach involves improper or unauthorised collection, use, disclosure, retention or disposal of personal information.

¹⁸ Article 34 (1) and (3).

¹⁹ Reynolds (2017), “GDPR matchup: US states data laws”, available [here](#), compares the GDPR and US state data breach laws. It found that many US states require notifications to data subjects on any breach when the data are not encrypted or the encryption key was compromised, irrespective of the degree of possible harm to data subjects. Conversely, the GDPR requires notifications to data subjects when the breach is likely to result in a high risk to the rights and freedoms of natural persons. Reynolds also mentions

that, in those US states with a harm threshold, the analysis of the risk focuses typically on financial harm, i.e. theft or fraud, or identity theft.

²⁰ Article 34(1) provides that: “When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.”

²¹ Article 2(1) provides that: “When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall, in addition to the notification referred to in Article 2, also notify the subscriber or individual of the breach.”

²² EDPB (2019), “1 year GDPR – taking stock”, available [here](#).

²³ FTC (2019), “Equifax to pay \$575 million as part of settlement with FTC, CFPB, and states related to 2017 data breach”, available [here](#).

²⁴ Law.com, 2019, “Equifax reaches \$1.4B data breach settlement in consumer class action”, available [here](#).

²⁵ Yahoo Data Breach Settlement.com, n.d., available [here](#).

²⁶ In October 2020, the Spanish Data Protection authority released [Comunica-Gap RGPD](#) to help organisations decide whether to inform individuals that they have suffered a data breach.