KOMMUNAL- OG
MODERNISERINGSDEPARTEMENTET

Retningslinjer OECD - 2013

OECDs retningslinjer for personvern og utveksling av personopplysninger over landegrenser

OECD

KOMMUNAL- OG
MODERNISERINGSDEPARTEMENTET

Retningslinjer OECD - 2013

OECDs retningslinjer for personvern og utveksling av personopplysninger over landegrenser

Kvaliteten på oversettelsen, og hvordan denne er i overensstemmelse med originalteksten, er Kommunal- og moderniseringsdepartementets ansvar. Dersom det er avvik mellom oversettelsen og originalteksten, er det ordlyden i originalteksten som skal legges til grunn.

Innhold

ANBEFALING FRA OECDS RÅD VEDRØRENDE RETNINGSLINJER FOR PERSONVERN OG UTVEKSLING AV PERSONOPPLYSNINGER OVER LANDEGRENSER

[C(80)58/FINAL, sist endret 11. juli 2013 [C(2013)79]

RÅDET,

SOM VISER TIL konvensjonen av 14. desember 1960 om Organisasjonen for økonomisk samarbeid og utvikling, artikkel 5 b);

SOM VISER TIL *Ministerial Declaration on the Protection of Privacy on Global Networks* [Vedlegg 1 til C(98)177]; *OECD retningslinjer for sikkerhet i informasjonssystemer og nettverk* [C(2002)131/FINAL], *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* [C(2007)67], *Declaration for the Future of the Internet Economy (The Seoul Declaration)* [C(2008)99], *Recommendation of the Council on Principles for Internet Policy Making* [C(2011)154], *Recommendation of the Council on the Protection of Children Online* [C(2011)155] og *Recommendation of the Council on Regulatory Policy and Governance* [C(2012)37];

SOM ERKJENNER at medlemsland har felles interesse i å fremme og beskytte de grunnleggende verdiene som ligger i personvern, individuelle friheter og fri flyt av opplysninger over landegrensene;

SOM ERKJENNER at en mer utvidet bruk og nye former for utnyttelse av personopplysninger gir større økonomiske og samfunnsmessige fordeler, men også medfører økt risiko for personvernet;

SOM ERKJENNER at en kontinuerlig flyt av personopplysninger i globale nettverk forsterker behovet for en bedre samordning av rammeverk for personvern, i tillegg til økt samarbeid mellom tilsynsmyndigheter over landegrensene;

SOM ERKJENNER viktigheten av risikovurderinger ved utforming av personvernpolitikk- og tiltak;

SOM ERKJENNER sikkerhetstruslene mot personopplysninger som eksisterer i åpne sammenkoblede omgivelser der personopplysninger i økende grad anses som et verdifullt gode;

SOM HAR BESLUTTET å videreutvikle fri informasjonsflyt mellom medlemsland og unngå å skape unødvendige hindre for økonomiske og samfunnsmessige bånd mellom dem;

Vedrørende forslaget til komiteen for informasjons-, data- og kommunikasjonspolitikk:

I. **ANBEFALER** at medlemsland:

- Utviser lederskap og forplikter seg til å beskytte personvernet og fri informasjonsflyt på høyeste nivå i statlig forvaltning;

- Gjennomfører retningslinjene i vedlegget til denne anbefalingen, som for øvrig utgjør en vesentlig del av denne, gjennom prosesser som omfatter alle aktuelle interessenter;

- Sprer denne anbefalingen i offentlig og privat sektor;

II. **OPPFORDRER** ikke-medlemmer til å følge anbefalingen og i samarbeid med medlemsland å iverksette den over landegrensene.

III. **INSTRUERER** Komiteen for informasjons-, data- og kommunikasjonspolitikk om å overvåke gjennomføringen av anbefalingen, vurdere informasjonen og rapportere til Rådet innen fem år etter at anbefalingen er vedtatt, og deretter ved behov.

Denne anbefalingen er en revisjon av Rådets anbefaling vedrørende *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, datert 23. september 1980 [C(80)58/FINAL].

VEDLEGG

RETNINGSLINJER FOR PERSONVERN OG UTVEKSLING AV PERSONOPPLYSNINGER OVER LANDEGRENSER

DEL I. GENERELT

Definisjoner

1. Følgende definisjoner gjelder:

   a) "behandlingsansvarlig" viser til den som i henhold til nasjonal lovgivning er kompetent til å bestemme innholdet og kontrollere bruken av personopplysninger, uavhengig av om de blir innhentet, lagret, behandlet eller videreformidlet av behandlingsansvarlig selv eller av en representant for denne;

   b) "personopplysninger" viser til opplysninger som knyttes til en identifisert eller identifiserbar enkeltperson (den registrerte);

   c) "personvernregelverk" viser til nasjonale lover eller forskrifter som beskytter personopplysninger, og som er i tråd med disse retningslinjene;

   d) "tilsynsmyndighet" viser til det offentlige organet i hvert medlemsland som har ansvar for å håndheve personvernregelverk, og som har fullmakt til å igangsette etterforskning og gi pålegg;

   e) "utveksling av personopplysninger over landegrenser" viser til flyt av personopplysninger på tvers av nasjonale grenser.

Virkeområde for retningslinjene

2. Retningslinjene gjelder for personopplysninger både i offentlig og privat sektor som på grunn av måten de behandles på, opplysningenes art eller sammenhengen de blir brukt i, representerer en risiko for personvernet og individuelle friheter.

3. Prinsippene i disse retningslinjene utfyller hverandre og skal leses i sammenheng. De skal ikke tolkes:

   a) slik at de hindrer iverksettelsen av ulike beskyttelsestiltak for ulike kategorier personopplysninger, avhengig av opplysningenes art og hvilken sammenheng de innhentes, lagres, behandles eller spres i, eller

   b) slik at de urettmessig begrenser ytringsfriheten.

4. Unntak fra disse retningslinjene, herunder de som har betydning for nasjonal suverenitet, nasjonal sikkerhet og samfunnsordenen ("*ordre public"),* skal være:

   a) så få som mulig, og

   b) gjøres kjent for offentligheten.

5. I forbundsstater kan overholdelse av retningslinjene bli berørt av maktfordelingen i forbundsstaten.

6. Retningslinjene skal anses som en minimumsstandard og kan suppleres med ekstra tiltak for å styrke personvernet og individuelle friheter, noe som kan virke inn på utvekslingen av personopplysninger over landegrensene.

DEL II. GRUNNLEGGENDE PRINSIPPER FOR NASJONAL ANVENDELSE

Innsamlingsbegrensninger

7. Det skal fastsettes begrensninger for innsamling av personopplysninger, og personopplysninger skal innhentes ved hjelp av lovlige og anerkjente metoder. Dersom det er formålstjenlig, skal den registrerte være informert om eller ha gitt sitt samtykke til innsamlingen.

Kvaliteten på opplysningene

8. Personopplysninger skal være relevante for formålet, og de skal være korrekte, fullstendige og oppdaterte i den grad det er nødvendig for formålet.

Formålspresisering

9. Formålet med innhenting av personopplysninger skal presiseres senest på det tidspunktet opplysningene samles inn. Etterfølgende bruk skal være begrenset til innsamlingsformålene eller til andre formål som ikke er uforenlige med disse, og som angitt i hvert enkelt tilfelle der formålet er endret.

Bruksbegrensninger

10. Personopplysninger skal ikke utleveres, gjøres tilgjengelige eller på andre måter benyttes til andre formål enn de som er angitt under § 9, unntatt:

    a) med samtykke fra den registrerte selv; eller

    b) med hjemmel i lov.

Sikkerhetstiltak

11. Personopplysninger skal beskyttes av rimelige sikkerhetstiltak mot risikofaktorer som tap eller uautorisert tilgang, ødeleggelse, bruk, endring eller utlevering.

Åpenhet

12. Det skal legges til grunn et generelt prinsipp om åpenhet om til utvikling, politikk og praksis knyttet til personopplysninger. Metoder for å fastslå eksistensen og arten av personopplysninger skal være lett tilgjengelige. Det samme gjelder innsamlingsformålene samt den behandlingsansvarliges identitet og normale tilholdssted.

Individuell deltakelse

13. Enkeltpersoner har rett til:

    a) å motta bekreftelse fra behandlingsansvarlig eller andre på om behandlingsansvarlig har opplysninger som knytter seg til dem;

    b) å bli meddelt disse opplysningene

        i. innen rimelig tid;

        ii. til en kostnad, hvis noen, som ikke er urimelig høy

iii. på en tilfredsstillende måte; og

iv. i et forståelig format ;

c) å motta begrunnelse dersom en forespørsel etter punkt (a) eller (b) blir avslått, og så å kunne påklage et slikt avslag; og

d) å kunne påklage behandling av opplysninger som knytter seg til dem, og hvis klagen fører frem, kunne få opplysningene slettet, rettet eller supplert.

Ansvar

14. Behandlingsansvarlig er pålagt å etterleve regler som gjennomfører prinsippene som er nevnt ovenfor.

DEL III. GJENNOMFØRING AV ANSVARSPRINSIPPET

15. En behandlingsansvarlig skal:

a) Ha på plass et internkontrollsystem for personopplysninger som:

i. gjennomfører disse retningslinjene for alle personopplysninger under dens kontroll;

ii. er skreddersydd virksomhetens struktur, størrelse, volum og sensitivitet;

iii. sørger for hensiktsmessige beskyttelsestiltak basert på en risikovurdering;

iv. er integrert i virksomhetens styringssystemer og etablerer interne kontrollrutiner;

v. inneholder planer for behandling av forespørsler og hendelser;

vi. er oppdaterte i lys av pågående kontroll og regelmessig evaluering;

b) Være beredt til å fremvise sitt internkontrollsystem ved behov, spesielt på forespørsel fra kompetent tilsynsmyndighet eller annet organ som er ansvarlig for å fremme bransjenormer eller liknende ordninger som gjennomfører disse retningslinjene; og

c) Melde fra til tilsynsmyndighet eller annen relevant myndighet ved behov og når det har forekommet et vesentlig sikkerhetsbrudd som påvirker personopplysninger. Dersom det er sannsynlig at sikkerhetsbruddet vil berøre de registrerte på en uheldig måte, skal den behandlingsansvarlige varsle de registrerte.

DEL IV. GRUNNLEGGENDE PRINSIPPER FOR INTERNASJONAL ANVENDELSE: FRI FLYT OG RETTMESSIGE RESTRIKSJONER

16. En behandlingsansvarlig er ansvarlig for de personopplysningene den har under sin kontroll, uavhengig av hvor opplysningene måtte befinne seg.

17. Et medlemsland skal ikke legge restriksjoner på utveksling av personopplysninger mellom seg og et annet land når (a) det andre landet i det alt vesentlige overholder disse retningslinjene, eller (b) det finnes tilstrekkelige sikkerhetstiltak, herunder effektive håndhevingsrutiner og hensiktsmessige ordninger gitt av behandlingsansvarlig, som sikrer et fortsatt tilfredsstillende beskyttelsesnivå i samsvar med disse retningslinjene.

18. Restriksjoner på utveksling av personopplysninger over landegrensene skal stå i forhold til risikoene ved slik utveksling, med hensyn til opplysningenes sensitivitet, behandlingsformål og sammenhengen behandlingen inngår i.

DEL V. NASJONAL GJENNOMFØRING

19. Når disse retningslinjene gjennomføres, skal medlemslandene:

    a) utvikle nasjonale personvernstrategier som gir uttrykk for en helhetlig tilnærming til personvernspørsmål i statlige organer;

    b) vedta personvernregelverk; etablere og opprettholde tilsynsmyndigheter som har kompetanse, ressurser og teknisk kunnskap til å utøve sin myndighet effektivt og kunne ta beslutninger på et objektivt, nøytralt og ikke-diskriminerende grunnlag;

    c) oppmuntre og støtte selvregulerende tiltak, det være seg bransjenormer eller annet;

    d) sørge for at enkeltpersoner har rimelig mulighet til å benytte seg av sine rettigheter;

    e) ha adekvate sanksjoner og virkemidler ved brudd på personvernregelverk;

    f) vurdere ytterligere tiltak, herunder drive opplysningsarbeid og bevisstgjøring, utvikle ferdigheter og stimulere til tekniske løsninger for å styrke personvernet;

    g) vurdere rollen til andre aktører enn den behandlingsansvarlige, i lys av den enkeltes rolle; og

    h) sørge for at de registrerte ikke opplever urettmessig diskriminering.

DEL VI. INTERNASJONALT SAMARBEID OG SAMORDNING

20. Medlemsland skal legge til rette for samarbeid om håndheving av personvernregelverk over landegrensene, særlig ved å forbedre informasjonsdeling mellom tilsynsmyndigheter.

21. Medlemsland skal oppfordre til, og støtte utforming av, internasjonale avtaler som fremmer samordning av rammeverk for personvern som gjennomfører disse retningslinjene.

22. Medlemsland skal oppfordre til at det utvikles internasjonalt sammenliknbare analysemetoder som kan gi bedre beslutningsgrunnlag for politiske prosesser om personvern og utveksling av personopplysninger over landegrensene.

23. Medlemsland skal offentliggjøre informasjon om hvordan de overholder disse retningslinjene.

TILLEGGSMEMORANDUM TIL REVIDERT RÅDSANBEFALING VEDRØRENDE RETNINGSLINJER FOR PERSONVERN OG UTVEKSLING AV PERSONOPPLYSNINGER OVER LANDEGRENSER

INNLEDNING

I 1980 vedtok OECD *Retningslinjer for personvern og utveksling av personopplysninger over landegrenser (*"retningslinjene av 1980") for å håndtere utfordringer knyttet til økt bruk av personopplysninger og trusselen mot globale økonomier når det legges restriksjoner på informasjonsflyt over landegrenser. Retningslinjene av 1980, som ga de første internasjonalt omforente personvernprinsippene, har påvirket lovgivning og politikk både i og utenfor OECD-landene. De er uttrykt i et presist og teknologinøytralt språk og har vist seg å være overraskende tilpasningsdyktige til teknologiske og samfunnsmessige endringer. Ikke desto mindre har endringer i bruk av personopplysninger og nye tilnærminger til personvern gjort at det er behov for oppdatering av retningslinjene av 1980 på en rekke viktige punkter. Michael Kirby var leder for den opprinnelige ekspertgruppen i OECD som laget utkastet til retningslinjene. Da dommer Kirby reflekterte over hva man hadde oppnådd i forbindelse med retningslinjenes 30-årsjubileum, konstaterte han: "På området informasjonspolitikk kan ingen internasjonale prinsipper forbli upåvirket av de voldsomme teknologiske endringene."[1]

Revisjonens kontekst

I løpet av de siste tretti årene har personopplysninger fått en stadig viktigere rolle i økonomien, i samfunnet og i dagliglivet. Nyskapninger, spesielt innenfor informasjons- og kommunikasjonsteknologi, har hatt stor påvirkning på næringsliv, offentlig forvaltning og enkeltmenneskers private aktiviteter. Nye teknologier og forsvarlig informasjonsbruk gir store økonomiske og samfunnsmessige fordeler. Mengden personopplysninger som hentes inn, brukes og lagres, er enorm, og vokser stadig. Moderne kommunikasjonsteknologi muliggjør voksende omfang av utveksling av opplysninger. Den potensielle bruken av personopplysninger har økt voldsomt på grunn av analysemetodene, som kan gi omfattende innsikt i enkeltmenneskers bevegelser, interesser og aktiviteter.

Samtidig medfører overfloden og varigheten av personopplysninger en økt trussel mot personvernet. Personopplysninger blir stadig oftere brukt på måter som ikke var forutsatt da opplysningene ble samlet inn. Nesten alle menneskelige aktiviteter etterlater seg digitale spor som gjør det stadig enklere å overvåke enkeltmenneskers atferd. Svikt i sikkerheten rundt personopplysninger er vanlig, og den økte risikoen signaliserer et behov for mer effektive tiltak for å beskytte personvernet.

De siste årene er det tatt en rekke initiativ for å motvirke nye og forhøyede risikofaktorer, særlig i sammenheng med utveksling av opplysninger over landegrensene. Arbeidet pågår, og eksempler omfatter EUs system med bindende foretaksregler ("Binding Corporate Rules", eller BCR)[2]; den globale diskusjonen om hvilke elementer man er enige om inngår i behandlingsansvaret[3]; og APECs regelverk for personvern over landegrenser (APEC CBPR).[4] I OECD har samarbeid mellom tilsynsmyndigheter over landegrensene hatt høy prioritet, noe som har resultert i vedtakelsen av *Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy* fra 2007 ("anbefalingen av 2007").[5]

Seoul Declaration for the Future of the Internet Economy (2008) anbefaler at OECD gjennomgår bruken av enkelte OECD-verktøy, herunder retningslinjene av 1980, i lys av "endrede teknologier, markeder og brukeratferd, og den økte betydningen av digitale identiteter". Erklæringen var den utløsende faktor for igangsettelse av en formell evaluering av retningslinjene av 1980.

OECD Recommendation on Principles for Internet Policy Making (2011)[6] etterlyste en mer konsekvent og effektiv beskyttelse av personvern på globalt nivå. Selv om OECDs retningslinjer for personvern har et bredere virkeområde enn internettpolitikk, er anbefalingen av 2011 ikke desto mindre nyttig. Kunngjøringen som er vedlagt anbefalingen av 2011 forklarer at dagens personvernutfordringer sannsynligvis vil bli mer akutte "ettersom økonomien og samfunnet i enda større grad er avhengig av en utvidet og innovativ bruk av personopplysninger, som enklere kan hentes inn, lagres og analyseres.".[7]

Rammeverk for personvern over hele verden blir nå gjennomgått og forbedret. Tre av de viktigste rammeverkene med internasjonalt tilsnitt (OECD, EU og Europarådet) har vært under revisjon samtidig, og et fjerde (APEC) holder på å innføre nye ordninger for utveksling av personopplysninger på tvers av landegrensene. Nasjonale rammeverk over hele verden blir også gjennomgått, fra Australia til Brasil, Kina og USA. I lys av denne utviklingen har OECD konkludert med at det nå er rette tidspunkt å gjennomføre en omfattende evaluering av retningslinjene av 1980.

Evalueringsprosessen

Forberedelser til evalueringen startet i 2010 i sammenheng med 30-årsjubileet for retningslinjene av 1980. Som en del av prosessen arrangerte OECD tre tematiske konferanser. De tok for seg (1) hvilken innflytelse retningslinjene av 1980 har hatt; (2) utviklingen av individets rolle; og (3) de økonomiske aspektene ved personopplysninger og personvern. Det ble også utarbeidet to rapporter: *The Evolving Privacy Landscape: 30 Years after the OECD Privacy Guidelines*[8], og *Implementation of the OECD Recommendation on Privacy Law Enforcement Co-operation*.[9]

Arbeidsgruppen for informasjonssikkerhet og personvern (WPISP) tok utgangspunkt i denne foreløpige rapporten og utarbeidet Referansevilkår[10] som et veikart for evalueringen. Referansevilkårene uttrykte en felles oppfatning av aktuelle utfordringer og tilnærminger, og utgjorde grunnlaget for det videre arbeidet. Foruten å sette fingeren på samfunnsendringer, fastslo referansevilkårene hva medlemslandene anså som vesentlig for å bedre personvernet.

En frivillig gruppe av personvereksperter ("ekspertgruppen") ble dannet for å bistå WPISP i evalueringsprosessen. Gruppen besto av eksperter fra regjeringer, tilsynsmyndigheter, akademia, næringslivet, sivilsamfunnet og teknologimiljøer. Deltakerne omfattet også representanter fra Europarådet og EU foruten eksperter fra APEC. Denne brede interessentgruppen ble ledet av Jennifer Stoddart, leder for den kanadiske personverntilsynsmyndigheten. Omer Tene fungerte som rådgiver for gruppen. Ekspertgruppen har samarbeidet gjennom en rekke møter og ved bruk av elektroniske møteplasser i løpet av 2011 og 2012. På møtene har det vært fokusert på tre hovedområder som referansevilkårene har blinket ut, nemlig: (1) nøkkelaktørenes roller og ansvarsområder; (2) geografiske begrensninger på datautveksling over landegrensene; og (3) proaktiv gjennomføring og håndhevelse.

Holdningen som ekspertgruppens arbeid signaliserte, var at selv om klimaet for personvern og utveksling av personopplysninger over landegrensene har endret seg vesentlig, var det ønskelig å oppdatere retningslinjene av 1980 i stedet for å gjøre en total revurdering av retningslinjenes grunnleggende prinsipper. Ekspertgruppen mente at balansen som gjenspeiles i de åtte hovedprinsippene i del II i retningslinjene av 1980, generelt sett er holdbare og bør bevares. Ekspertgruppen innførte en rekke nye konsepter i OECDs rammeverk for personvern, herunder internkontroll, varsling om sikkerhetsbrudd, nasjonale strategier for personvern, samt opplæring, bevisstgjøring og global samordning. Andre sider ved retningslinjene av 1980 ble utvidet og oppdatert, blant annet ansvarsprinsippet, utveksling av personopplysninger over landegrensene og håndhevelse av personvernreglene.

Retningslinjene av 1980 hadde et memorandum som beskrev omstendighetene rundt tilblivelsen, samt den underliggende begrunnelsen for å utarbeide dem. Memorandumet gir oversikt over konkurrerende prioriteringer på den tiden og har en detaljert tolkning av ulike bestemmelser i retningslinjene av 1980,

hvorav noen ikke er blitt justert (spesielt de som står nevnt i del II). Disse vurderingene er fortsatt gyldige i dag. Tilleggsmemorandumet er utarbeidet som en del av evalueringsprosessen og skal følge de reviderte retningslinjene. Hensikten er å supplere – ikke erstatte – det opprinnelige memorandumet. Der det er gjort endringer i retningslinjene av 1980, kaster dette tilleggsmemorandumet lys over begrunnelsen for endringene og den nødvendige konteksten, for å gjøre det enklere å forstå og tolke dem.

REVISJON AV RETNINGSLINJENE

Internkontroll

Del II i retningslinjene av 1980 fastsetter ansvarsprinsippet, som plasserer ansvaret for å etterleve "tiltak som gjennomfører de resterende prinsipper" hos den behandlingsansvarlige. Erkjennelsen av ansvarsprinsippets betydning er blitt større de siste årene. Nasjonale personvernregler har etter hvert innført en rekke ordninger som aktivt støtter ansvarsprinsippet både blant offentlige og private behandlingsansvarlige. Forpliktelse til åpenhet overfor enkeltpersoner og tilsynsmyndigheter er tydelige eksempler på slike ordninger.

De siste årene har ansvarsprinsippet fått fornyet oppmerksomhet som et verktøy til å underbygge og definere et virksomhetsansvar for personvernet. På bakgrunn av denne erfaringen introduserer den nye del III i retningslinjene (*Gjennomføring av ansvarsprinsippet*) ideen om internkontroll, og formulerer de viktigste punktene i denne.

§ 15 (a) (i) slår fast at internkontrollen hos en behandlingsansvarlig skal gjennomføre retningslinjene for alle personopplysninger som han er ansvarlig for. Begrepet "ansvar" viser tilbake til definisjonen av "behandlingsansvarlig", som angitt i § 1 (a). Formuleringen understreker at internkontrollen ikke bare skal gjelde for den behandlingsansvarliges egen virksomhet, men for all virksomhet den kan stilles til ansvar for – uavhengig av hvem opplysningene er overført til. Internkontrollen skal for eksempel omfatte rutiner som sikrer at representanter for den behandlingsansvarlige opprettholder nødvendige sikkerhetstiltak når de behandler personopplysninger på vegne av denne. Sikkerhetstiltak kan også være nødvendig ved samarbeid med andre behandlingsansvarlige, særlig der ansvaret for å gjennomføre retningslinjene er delt. Slike sikkerhetstiltak kan innbefatte kontraktsvilkår som gjelder etterlevelse av den behandlingsansvarliges personvernpolitikk- og praksis, systemer for å varsle behandlingsansvarlige i tilfelle sikkerhetsbrudd, skolering og opplæring av medarbeidere, vilkår for bruk av underleverandører og rutiner for å gjennomføre granskninger.

§ 15 (a) (i) viser bare til retningslinjene som en kilde til regler eller prinsipper som skal gjennomføres ved hjelp av internkontroll. I praksis kan slike planer også måtte avspeile andre kilder; iberegnet nasjonale regelverk, internasjonale forpliktelser, selvreguleringsmekanismer og kontraktsvilkår.

§ 15 (a) (ii) understreker nødvendigheten av fleksibilitet ved innføring av internkontroll. Store behandlingsansvarlige som er etablert i flere jurisdiksjoner, kan ha behov for andre interne kontrollrutiner enn små og mellomstore virksomheter som er etablert på ett sted. Samtidig slås det fast i § 15 (a) (ii) at internkontroll må tilpasses volumet og sensitiviteten til den behandlingsansvarliges drift. Internkontroll hos behandlingsansvarlige som håndterer personopplysninger i stort volum, må være mer omfattende enn hos dem som bare behandler begrensede mengder personopplysninger. Hvor sensitive personopplysninger som behandles, kan også ha betydning for utformingen av internkontrollen, fordi også en liten behandlingsansvarlig kan håndtere svært sensitive personopplysninger.

Et tilbakevendende tema i diskusjonene om internkontroll var behovet for å kunne benytte internkontroll til å utvikle hensiktsmessige sikkerhetstiltak basert på en risikovurdering av personvernet. § 15 (a) (iii) sier at

nødvendige sikkerhetstiltak må bestemmes med grunnlag i en prosess som kartlegger, analyserer og vurderer risikofaktorer knyttet til enkeltpersoners personvern. Enkelte ganger foregår prosessen slik at man foretar en analyse av personvernkonsekvenser før internkontroll eller andre tiltak settes ut i livet, eller før det gjøres vesentlige endringer i behandlingen av personopplysninger. "Risiko" er ment å være et vidt begrep som tar høyde for en rekke mulige skadeeffekter for enkeltpersoner. En internkontroll kan også bidra til praktisk gjennomføring av ideer som "innebygd personvern", der personvernvennlige teknologier, prosesser og rutiner bygges inn i systemarkitekturer i stedet for å legges til i etterkant.

§ 15 (a) (iv) peker på at internkontroll må integreres i styringsstrukturen til den behandlingsansvarlige og etablere hensiktsmessige kontrollrutiner internt. Det er svært viktig at toppledelsen forplikter seg og gir sin støtte til planen så den får en vellykket gjennomføring. Tilstrekkelig med ressurser og personell, samt opplæringstiltak, vil også kunne bidra til en mer effektiv internkontroll. Personvernrådgivere vil kunne spille en viktig rolle i utformingen og gjennomføringen av internkontrollen.

§ 15 (a) (v) slår fast at internkontrollen også skal ha rutiner for håndtering av hendelser og forespørsler. Den økte forekomsten av sikkerhetsbrudd som berører personopplysninger, viser hvor viktig det er å utarbeide en plan for hendelsesrespons som omfatter varsling om sikkerhetsbrudd (se nedenfor). For å støtte opp om "Individuell deltakelse" i del II skal behandlingsansvarlige også svare på henvendelser (enten i form av klager eller informasjonsforespørsler) fra de registrerte i rett tid. Endelig slår § 15 (a) (vi) fast at internkontrollen skal gjennomgås rutinemessig og oppdateres for å sikre at de fremdeles er tilpasset den aktuelle risikosituasjonen.

§ 15 (b) slår fast at en behandlingsansvarlig skal kunne dokumentere internkontrollen ved behov, særlig på forespørsel fra tilsynsmyndighet eller annet organ som er ansvarlig for å fremme etterlevelse av bransjenormer eller andre ordninger som gjør disse retningslinjene gjeldende. Ved å gi internkontrollen tilstrekkelig slagkraft og effekt ansvarliggjøres den behandlingsansvarlige, også når det ikke har forekommet sikkerhetsbrudd eller påstander om avvik. En evaluering av internkontrolldokumentasjonen kan foretas av tilsynsmyndigheten eller av en representant for denne.

§ 15 (b) innholder begrepene "ved behov" og "kompetent" for å understreke at behandlingsansvarlige skal kunne dokumentere internkontrollen på forespørsel fra en tilsynsmyndighet med nødvendig jurisdiksjon. Retningslinjene regulerer ikke spørsmål om jurisdiksjon, kompetanse eller lovvalg.

Internkontrolldokumentasjon kan også fremlegges for et organ med ansvar for å fremme etterlevelse av bransjenormer eller liknende ordninger som gjennomfører disse retningslinjene. Ordningene kan omfatte merkeordninger eller sertifiseringssystemer og kan også gjelde utveksling av personopplysninger over landegrensene. I dette henseendet kan det bemerkes at § 21 oppfordrer til internasjonale ordninger som gjennomfører retningslinjene. EUs bindende foretaksregler (BCR) og APECs regelverk for internasjonalt personvern representerer to modeller for en slik ordning.

Varsel om brudd på datasikkerhet

Av "Sikkerhetstiltak" i del II følger at "Personopplysninger skal beskyttes av rimelige sikkerhetstiltak mot risikofaktorer som tap eller uautorisert tilgang, ødeleggelse, bruk, endring eller utlevering". En rekke høyprofilerte sikkerhetsbrudd har vist at sikkerhet ved behandling av personopplysninger fremdeles representerer en utfordring.

Sikkerhetsbrudd kan for eksempel forekomme når uforsiktige medarbeidere utfører handlinger som ikke er i tråd med rutinene, hackere får tilgang til databaser som ikke er godt nok beskyttet, eller tyver ser sitt snitt til å stjele usikret bærbart datautstyr. De underliggende årsakene – manglende opplæring og bevissthet hos ansatte, utdaterte sikkerhetstiltak, mangelfull tilgangsstyring, innsamling av for mye data og uspesifisert lagringstid eller mangel på kontrollrutiner – kan imidlertid ofte tilskrives behandlingsansvarlig.

Misbruk av personopplysninger kan påføre enkeltpersoner potensielt stor skade, uavhengig av om det skyldes uforvarende tap eller bevisst tyveri. Virksomheter som opplever sikkerhetsbrudd, pådrar seg ofte betydelige kostnader når de skal svare på hendelsen, finne årsaken til den og iverksette tiltak for å forhindre at hendelsen gjentar seg. Dette kan også påvirke deres omdømme i betydelig grad. Tap av tillit kan få alvorlige følger for organisasjoner. Derfor er sikring av personopplysninger blitt et svært viktig tema for forvaltningen, næringslivet og enkeltpersoner.

Lovbestemmelser om varsling av sikkerhetsbrudd som krever at den behandlingsansvarlige informerer enkeltpersoner og/eller myndigheter når slike brudd oppstår, er vedtatt eller foreslått i mange land. Begrunnelsen for slike bestemmelser er vanligvis at behandlingsansvarlige har få insentiver til frivillig å avdekke brudd siden dette kan være skadelig for deres omdømme. Ved å kreve varsling kan enkeltpersoner ta forholdsregler for å beskytte seg mot følgene av identitetstyveri eller andre skader. Krav om varsling kan også gi tilsynsmyndigheter eller andre myndigheter opplysninger som kan avgjøre om hendelsen skal etterforskes, eller om det skal iverksettes andre tiltak. Ideelt sett vil regler om varsling av sikkerhetsbrudd også motivere behandlingsansvarlige til å iverksette hensiktsmessige tiltak for å sikre personopplysningene de har ansvar for.

Foruten å bidra til datasikkerhet, vil varsling om brudd styrke andre grunnleggende prinsipper i retningslinjenes del II, herunder prinsippene om ansvar, individuell deltakelse og åpenhet. Videre vil obligatorisk varsling kunne gi bedre dokumentasjonsgrunnlag for å utforme regelverk om personvern og informasjonssikkerhet ved å frembringe opplysninger om antall, alvorlighetsgrad og årsaker til sikkerhetsbruddene.

Sikkerhetsbrudd er ikke bare en utfordring for personvernet, men berører også andre spørsmål, blant annet strafferettspleie og informasjonssikkerhet. Når en virksomhet rammes av sikkerhetsbrudd, i særdeleshet hvis den skyldes eksternt angrep, kan det være hensiktsmessig eller påkrevd å melde fra om bruddet til andre myndigheter enn tilsynsmyndigheten (eksempelvis responsteam for datahendelser, påtalemyndigheten eller andre organer med overordnet ansvar for informasjonssikkerhet).

Kreves det varsling for alle sikkerhetsbrudd, uansett hvor små, kan dette være en uforholdsmessig stor belastning for behandlingsansvarlige og tilsynsmyndigheter. Dessuten vil overdreven varsling til de registrerte kunne medføre at de ignorerer meldingene. Følgelig har den nye bestemmelsen i retningslinjene [§ 15 (c)] en risikobasert tilnærming til varsling. Varsling er påkrevd der det foreligger et "vesentlig sikkerhetsbrudd som påvirker personopplysninger", en formulering som er ment å dekke brudd som setter personvernet og individuelle friheter i fare. Dersom det er sannsynlig at et sikkerhetsbrudd vil berøre enkeltpersoner på en uheldig måte, er det formålstjenlig også å varsle disse. For å avgjøre om det er sannsynlig at et brudd vil berøre de registrerte "på en uheldig måte", bør "uheldig" tolkes vidt og omfatte også andre faktorer enn økonomisk tap. Varslingskravene bør være fleksible for å forhindre eller begrense ytterligere skade. Det kan forekomme situasjoner der varsling til de registrerte ikke er hensiktsmessig, for eksempel når det medfører økt risiko for de registrerte eller hindrer etterforskning av lovbrudd.

Eksisterende regler om varsling av sikkerhetsbrudd varierer med hensyn til varslingsterskel, hvilke parter som skal varsles, tidspunkt for varsling, og rollen til tilsynsmyndighet og andre myndigheter. Det kan være nødvendig å samle ytterligere erfaringer for å avgjøre hvilke typer varsling som er mest effektive i praksis.

Sikkerhetsbrudd kan påvirke personopplysninger til enkeltpersoner som bor i ulike jurisdiksjoner. Når krav til varsling blir utformet, iverksatt eller revidert, bør interessene til berørte personer som bor utenfor den aktuelle jurisdiksjonen, vies spesiell oppmerksomhet. I særdeleshet kan det være fordelaktig å varsle tilsynsmyndigheter i andre land der det er kjent eller anses som trolig at et betydelig antall enkeltpersoner er berørt. Ordninger for å håndheve regler over landegrensene er en metode for å understøtte eller spre varsler om viktige sikkerhetsbrudd til flere lands myndigheter. Slike ordninger kan også bidra til å sette fokus på utfordringer som oppstår som følge av motstridende rettslige krav.

Tilsynsmyndigheter

Verken retningslinjene av 1980 eller anbefalingen av 2007 krever eksplisitt at det etableres tilsynsmyndigheter, selv om sistnevnte forutsetter deres eksistens og anbefaler at de får den nødvendige makt og myndighet. De reviderte retningslinjene definerer og uttrykker i klartekst behovet for å etablere og opprettholde "tilsynsmyndigheter". De definerer også "personvernregelverk" som "nasjonale lover eller forskrifter som beskytter personopplysninger, og som er i tråd med disse retningslinjene". Begge definisjoner gjenspeiler de omforente definisjonene i anbefalingen av 2007.

Definisjonene av "personvernregelverk" og "tilsynsmyndigheter" gir rom for fleksibel bruk. "Personvernregelverk" viser ikke bare til generelle regler om personvern som er vanlig i medlemslandene, men også til sektorspesifikke personvernbestemmelser (f.eks. regler for kredittopplysningsvirksomhet eller i telekomsektoren) eller andre typer regulering som inneholder bestemmelser om beskyttelse av personopplysninger, og som således gjennomfører disse retningslinjene (f.eks. forbrukervernregulering). Likeledes viser "tilsynsmyndigheter" ikke bare til offentlige organer hvis hovedoppgave er å håndheve nasjonalt personvernregelverk, men kan eksempelvis også utvides til å gjelde regulatører som beskytter forbrukere, under forutsetning av at de har myndighet til å gjennomføre tilsyn eller iverksette tiltak som faller inn under håndheving av "personvernregelverk".

En ny bestemmelse i del V (*Gjennomføring nasjonalt*) krever at medlemsland etablerer og opprettholder tilsynsmyndigheter som har kompetanse, ressurser og teknisk ekspertise til å utøve sin myndighet effektivt, og til å kunne ta beslutninger på et "objektivt, nøytralt og ikke-diskriminerende grunnlag". Denne formuleringen er hentet fra OECDs anbefaling om politisk regulering og styring.[11] I retningslinjene henspiller den på at tilsynsmyndigheter skal være frie og uavhengige av politiske føringer, og uten kryssende interesser i sin håndheving av personvernregelverk. Det finnes en rekke virkemidler i de forskjellige medlemsland som sikrer at tilsynsmyndigheter er tilstrekkelig upartiske. § 19 (c) fokuserer på den praktiske effekten av slike virkemidler, som skal sørge for at tilsynsmyndigheter tar beslutninger på fritt grunnlag så det ikke kan stilles spørsmål ved deres faglige vurderinger, objektivitet eller integritet.

I enkelte land kan begrepet "tilsynsmyndighet" også vise til en gruppe organer som i felleskap står for håndhevingen av personvernregelverk. For eksempel kan tilsyn med behandlingsansvarlige i offentlig sektor involvere flere organer fra ulike deler av statsforvaltningen som også kan ha myndighet til å gi retningslinjer eller sette andre vilkår for bruk av opplysninger. "Kompetanse, ressurser og teknisk ekspertise" som forutsettes i § 19 (c), behøver i slike tilfeller ikke å være sentralisert til ett enkelt organ, men kan forefinnes i håndhevingsapparatet under ett.

Anbefalingen av 2007 understreket behovet for at tilsynsmyndigheter får de ressurser og den myndighet som er nødvendig for å (a) forebygge, hindre og sanksjonere brudd på personvernregelverket; (b) føre tilsyn, herunder få tilgang til relevant informasjon om mulige lovbrudd for å muliggjøre etterforskning; og (c) gjøre det mulig å iverksette korrigerende tiltak mot behandlingsansvarlige som er skyldige i slike brudd. Tilsynsmyndighetenes ressurser skal stå i rimelig forhold til omfanget og kompleksiteten av deres tilsynsoppgaver. Den nye bestemmelsen forutsetter også at tilsynsmyndigheter får tilstrekkelig teknisk kompetanse, noe som er avgjørende i lys av den økende kompleksiteten i databruken. Dette forsterker den nye trenden hos tilsynsmyndigheter til å ansette personale med teknisk bakgrunn.

Utveksling av personopplysninger over landegrenser

Da retningslinjene av 1980 ble utarbeidet, bestod utveksling av opplysninger for det meste av avgrensede ende-til-ende-overføringer mellom virksomheter eller forvaltning. I dag kan data prosesseres parallelt på flere steder, de kan spres og lagres over hele verden, i løpet av kort tid kobles sammen på nye måter, og forflyttes over landegrensene av enkeltpersoner med mobile enheter. Tjenester som "nettsky" gjør det

mulig for organisasjoner og enkeltpersoner å få tilgang til opplysninger som kan være lagret hvor som helst i verden.

Retningslinjene av 1980 forutsatte at overføring av opplysninger skulle være tillatt, men erkjente at stater måtte kunne sette begrensninger i visse tilfeller, som der mottakerlandet "ennå ikke i særlig grad overholder disse retningslinjene, eller der videreformidling av slike data ville innebære en omgåelse av landets interne personvernregelverk." Siden den gang har medlemsland etablert en rekke ulike ordninger for å beskytte enkeltpersoner i sammenheng med utveksling av opplysninger over landegrensene. Noen av disse ordningene omfatter en landsspesifikk evaluering, for eksempel "adekvansmodellen", vedtatt i EU. Andre ordninger baserer seg ikke på en landsspesifikk vurdering, men heller på sikkerhetstiltak utformet av behandlingsansvarlige. Slike ordninger omfatter for eksempel bindende foretaksregler (BCR), kontraktsmaler og grenseoverskridende personvernregler.

Endringene i del IV søker å forenkle og samle OECDs holdning til utveksling av personopplysninger over landegrensene. Den begynner med å stadfeste at en behandlingsansvarlig forblir ansvarlig for de personopplysningene den har under sin kontroll, uansett hvor opplysningene måtte befinne seg [§ 16]. Denne paragrafen gjentar det grunnleggende ansvarsprinsippet i del II, sett i sammenheng med utveksling av opplysninger over landegrensene. Utveksling av personopplysninger til land både innenfor og utenfor OECD medfører risiki som behandlingsansvarlige må håndtere. Enkelte utvekslinger krever nøye oppfølging på grunn av opplysningenes sensitivitet eller fordi mottakerlandet enten mangler vilje eller evne til å iverksette personverntiltak.

Uten å utelukke anvendelsen av § 6, beskriver § 17 to situasjoner der et medlemsland bør avstå fra å ilegge restriksjoner på utveksling av personopplysninger over landegrensene. § 17 (a) holder fast på den generelle oppfatningen i retningslinjene av 1980 og fastslår at medlemsland bør avstå fra å legge restriksjoner på utveksling av personopplysninger mellom seg og et annet land, dersom det andre landet i alt vesentlig overholder disse retningslinjene. § 17 (b) fraråder restriksjoner der det finnes tilstrekkelige tiltak som sikrer et beskyttelsesnivå i samsvar med disse retningslinjene. Den anerkjenner tiltak som behandlingsansvarlig kan iverksette for å sikre at beskyttelsesnivået opprettholdes. Tiltak kan være en kombinasjon av flere, for eksempel tekniske og organisatoriske sikringstiltak, kontrakter, prosedyrer for klagebehandling, kontrollrutiner etc. De tiltak som iverksettes av den behandlingsansvarlige, må imidlertid være tilstrekkelige, og de må suppleres med ordninger som gir effektiv håndheving dersom tiltakene skulle vise seg ineffektive. § 17 (b) forutsetter derfor at det finnes effektive virkemidler for håndheving som støtter de tiltakene behandlingsansvarlig har vedtatt. Slike virkemidler kan ha ulike former, herunder administrativ og rettslig håndheving i tillegg til samarbeid mellom tilsynsmyndigheter over landegrensene.

§ 16 og 17 er uavhengig av hverandre. Om det eksisterer eller ikke eksisterer nasjonale restriksjoner etter vedtak i henhold til § 17, påvirker som sådan ikke gjennomføringen av prinsippet i § 16 om at behandlingsansvarlige forblir ansvarlige for opplysninger under deres kontroll, også ved utveksling over landegrensene.

§ 18 oppdaterer språket i retningslinjene av 1980 slik at de henviser til "risiko" og "forholdsmessighet" for å angi at restriksjoner på utveksling av personopplysninger ilagt av medlemsland må stå i forhold til risikoen ved utveksling og ta hensyn til opplysningenes sensitivitet, behandlingsformål og sammenhengen behandlingen inngår i. Således er teksten blitt endret og har kommet mer på linje med andre bestemmelser i retningslinjene, som legger til grunn en risikobasert tilnærming.

§ 6 i retningslinjene anerkjenner medlemslandenes rett til å supplere retningslinjenes standarder med tiltak som er nødvendige for å beskytte personvernet og individuelle friheter, noe som kan ha innvirkning på utveksling av personopplysninger over landegrensene. Virkemidler av denne typen bør gjennomføres på en slik måte at de påvirker den frie flyten av personopplysninger minst mulig.

Nasjonal gjennomføring

Med hensyn til nasjonal gjennomføring fokuserte retningslinjene av 1980 på behovet for "rettslige, administrative og andre prosedyrer eller institusjoner". Selv om retningslinjene av 1980 også la vekt på ikke-rettslige tiltak, herunder selvregulering, erkjente man at det er nødvendig med flere virkemidler for å beskytte personvernet.

§ 19 (a) anbefaler at medlemsland utarbeider en nasjonal strategi for personvern som gjenspeiler en helhetlig tilnærming i forvaltningen. Å løfte personvernets betydning opp på høyeste nivå i statlig forvaltning bidrar til å styrke beskyttelsen av personvernet. En annen faktor er koordinering på tvers av statlige organer. Som det påpekes i OECDs *Recommendation on Regulatory Policy and Governance*, bør medlemsland aktivt støtte ensartet regeletterlevelse på ulike nivåer i forvaltningen. Der statlige myndigheter utformer en politikk for privat sektor, er det å sikre en koordinering mellom departementer og etater en nødvendig del av den nasjonale strategien. Dessuten er det mange offentlige organer som benytter seg av personopplysninger, og en annen side ved koordineringen er derfor å sørge for et enhetlig beskyttelsesnivå i de ulike organene. Endelig er en nasjonal strategi for personvern også et verktøy som sikrer ensartethet ved politikkutforming på beslektede områder (f.eks. nasjonal strategi for informasjonssikkerhet).

§ 19 (g) forutsetter at medlemsland vurderer ekstra tiltak, herunder å drive opplysningsarbeid og bevisstgjøring, kunnskapsutvikling og å stimulere til tekniske løsninger for å beskytte personvernet. Selv om det allerede finnes initiativ for å øke bevisstheten rundt personvern, er det bred enighet om at mer må gjøres på dette feltet. Referansevilkårene for evalueringen av retningslinjene etterlyser en kultur for personvern i organisasjoner og blant enkeltpersoner, noe som kan oppnås ved å styrke kunnskapen om personvern. Nye OECD-regler på beslektede områder omfatter opplæringstiltak og bevisstgjøring som del av rammeverket[12]. Slike initiativ bør omfatte et bredt utvalg aktører, herunder forvaltningsorganer, tilsynsmyndigheter, selvregulerende organer, organisasjoner i det sivile samfunn og lærere. Barn er en særdeles sårbar kategori registrerte, og medlemsland blir derfor spesielt oppfordret til å vurdere opplysningskampanjer som kan gi barn de nødvendige kunnskaper og ferdigheter til trygg bruk av internett, og kunne bruke nettet til sin fordel.

Fagpersoner med personvernkompetanse spiller en stadig viktigere rolle når det gjelder å gjennomføre og administrere internkontroll på personvernområdet. Flere medlemsland har allerede tatt initiativ til å definere kompetanseområder for personvernspesialister. Kompetansegivende kurs i beskyttelse av opplysninger og personvern i tillegg til spesialist- og videreutdanning kan bidra til å styrke ferdighetene på området. § 19 (g) oppfordrer medlemsland til særskilt å vurdere tiltak for å støtte slik kompetanseutvikling.

Tekniske tiltak spiller også en stadig større rolle som supplement til personvernregelverk. § 19 (g) foreslår tiltak som fremmer utviklingen og utbredelsen av personvernfremmende teknologier (PET). Medlemsland kan for eksempel velge å støtte utviklingen av tekniske standarder som støtter opp under personvernprinsippene. Initiativ for internasjonal standardisering kan også bringe den tekniske samordningen mellom personvernfremmende teknologier et skritt videre, noe som igjen kan bidra til større utbredelse av slike teknologier. Godkjennings- og merkeordninger vil ytterligere kunne fremme bruken av personvernfremmende teknologier. Andre tiltak omfatter forskning og utvikling, formidling av bransjenormer og veiledninger til regelverk.

§ 19 (h) innbyr medlemsland til å vurdere rollen til andre aktører enn de behandlingsansvarlige, ”i lys av den enkeltes rolle”. Under diskusjonen om behovet for ekstra tiltak ble det erkjent at andre aktører, selv om de ikke faller innunder begrepet behandlingsansvarlig, spiller en viktig rolle i fastsettelsen av beskyttelsesnivået for personopplysninger. I løpet av de siste årene har enkeltpersoner vokst ut av rollen som passive ”registrerte” og blitt aktive deltakere i prosessen med å skape, poste og dele opplysninger om seg selv, venner, familiemedlemmer og andre i et mangfold av informasjonskanaler, blant annet i sosiale nettverk, ratingsystemer og geolokaliseringsapplikasjoner. Da denne utviklingen ble diskutert, erkjente man at ikke

alle aktører nødvendigvis må reguleres på samme måte. Enkeltpersoner som handler som privatpersoner vil for eksempel vanligvis anses å falle utenfor retningslinjenes virkeområde, da relasjoner mellom individer som oftest er grunnleggende forskjellig fra relasjoner mellom enkeltpersoner og virksomheter. Ikke-rettslige tiltak, herunder opplæring og bevisstgjøringstiltak, ble ansett som mer hensiktsmessige for å imøtegå personvernrisikoene som knytter seg til enkeltpersoners aktiviteter. Der en enkeltperson forårsaker skade på andres personvern, kan erstatnings- eller sivilrettslige tiltak være en mulig løsning, men det kan også være behov for å vurdere andre tiltak.

Internasjonalt samarbeid og samordning

OECDs Anbefaling om prinsipper for en internettpolitikk (2011) etterlyste en mer enhetlig tilnærming til personvern og mer effektiv gjennomføring på globalt nivå. Kunngjøringen som er vedlagt Anbefalingen er ment å gi ytterligere informasjon og erkjenner staters målsetting om å få til en global samordning på området. Referansevilkårene har også erkjent verdien av et samordnet rammeverk for personvern på globalt nivå som sikrer effektiv beskyttelse og støtter opp om fri flyt av personopplysninger verden over. Som det imidlertid er skissert i Deauville-erklæringen (G8), står vi fremdeles overfor "betydelige utfordringer med hensyn til samordning og enhetlig utforming av offentlig politikk om temaer som personopplysningsvern".[13]

§ 21 formulerer medlemslandenes generelle målsetting om å få til en bedre samordning av rammeverk for personvern globalt gjennom internasjonale ordninger for gjennomføring av retningslinjene. Det finnes ulike tilnærminger til samordning av slike rammeverk. Safe Harbour-reglene mellom USA og EU[14], som ble vedtatt i samsvar med EUs adekvansregler og gjennomført i 2000, er et tidlig eksempel. Siden den gang er det tatt flere initiativ til å samkjøre ulike tilnærminger og systemer for beskyttelse, herunder arbeid som er gjort av tilsynsmyndigheter innenfor EUs ordning med bindende foretaksregler (BCR) og APECs regler om personvern over landegrenser i Asia- og Stillehavsregionen. Samtidig med at disse reviderte retnings-linjene blir publisert, er Europarådet i gang med å vurdere en modernisering av Konvensjon 108 om automatisert behandling av personopplysninger. Ytterligere arbeid er nødvendig på policynivå for å få en mer enhetlig tilnærming til internasjonal personvernregulering.

Et sterkt globalt nettverk av tilsynsmyndigheter som arbeider sammen, er et første viktig skritt mot global samordning. I 2005 tok OECD opp igjen spørsmål om globalt samarbeid mellom tilsynsmyndigheter, noe som resulterte i vedtaket om et nytt rammeverk for samarbeid over landegrenser i anbefalingen av 2007. Treårsrapporten om implementering av anbefalingen av 2007 understreket behovet for ytterligere innsats for å sikre at tilsynsmyndigheter har nødvendig kompetanse til å iverksette effektive sanksjoner og nok ressurser til å utføre sine oppgaver.[15] Referansevilkårene for evaluering av retningslinjene etterlyste en styrking av innsatsen for å utvikle et globalt og aktivt nettverk av tilsynsmyndigheter. § 20 repeterer forpliktelsen formulert av medlemslandene i anbefalingen av 2007 til å bedre samarbeidet mellom tilsyns-myndigheter. Medlemsland blir særskilt oppfordret til å imøtegå hindringer – det være seg juridiske eller praktiske – som står i veien for informasjonsdeling mellom tilsynsmyndigheter, slik at det kan legges til rette for en koordinert og effektiv håndheving. Å bryte ned barrierer for informasjonsdeling har vært viktig i denne sammenheng.

Å styrke den globale samordningen mellom tilsynsmyndigheter byr på utfordringer, men har fordeler som strekker seg mye lengre enn til å utveksle personopplysninger over landegrensene. Global samordning kan lette virksomheters regeletterlevelse og sørge for at kravene til personvern blir oppfylt. Det kan også øke enkeltpersoners bevissthet og forståelse rundt de rettigheter de har i en globalisert verden.

Bedre grunnlag for politiske beslutninger

OECDs anbefaling om en internettpolitikk etterlyser offentlig tilgjengelig og pålitelig informasjon som kan legges til grunn i regelverksarbeidet. Kunngjøringen som følger med anbefalingen, nevner spesielt nytten av internasjonalt sammenliknbare måleverktøy.

Dokumentasjonsgrunnlaget som for tiden er tilgjengelig ved regelverksutvikling på personvernområdet er ujevnt. Undersøkelser gjennomført av nasjonale statistiske byråer gir en viss innsikt i personvernspørsmål basert på internasjonalt sammenliknbare måleverktøy. Nedslagsfeltet for disse undersøkelsene, som først og fremst fokuserer på hvor bevisste enkeltpersoner er med hensyn til personvern, er imidlertid begrenset. Det er for eksempel hull knyttet til tekniske og økonomiske sider ved personvernet, i tillegg til gjennomføringen av forebyggende tiltak. Tilsynsmyndigheter samler betydelige mengder data som blir offentliggjort i årlige rapporter, men de er ikke i et format som egner seg for internasjonale sammenlikninger. For eksempel kunne en bedre forståelse av klageopplysninger, statistikk om sikkerhetsbrudd og hvordan økonomiske og andre sanksjoner påvirker behandlingsansvarliges atferd, vært en potensielt god kilde til kunnskap for de som skal utarbeide regelverk. Tilføyelsen av § 22 i del VI fastslår behovet for at medlemslandene støtter initiativ for å bedre beslutningsgrunnlaget på området.

Andre oppdateringer

I tillegg til de større endringene som er diskutert i forrige del, gjenspeiler de reviderte retningslinjene flere mindre endringer som enten er gjort for å bedre lesbarheten eller på andre måter oppdaterer språket i retningslinjene av 1980.

Generelt er alle referanser til bestemte deler av retningslinjene blitt erstattet med et mer generisk uttrykk ("disse retningslinjene").

§ 2, som spesifiserer virkeområdet for retningslinjene, henviser nå til ”risiko” i stedet for ”fare” for personvernet og individuelle friheter, noe som gjenspeiler at det er lagt større vekt på risiko i de reviderte retningslinjene. Endringen må ikke oppfattes slik at den hindrer medlemslandene i å utvide virkeområdet for personvernregelverket til å omfatte alle former for behandling av personopplysninger.

Tidligere § 3 (b) er fjernet, da muligheten medlemsland har til å holde "personopplysninger som ikke representerer en risiko for personvernet og individuelle friheter" utenfor retningslinjenes virkeområde, allerede er behandlet i § 2.

Tidligere § 3 (c) er fjernet, da medlemsland generelt sett har utvidet virkeområdet for nasjonale personvernregler til også å omfatte behandling av personopplysninger generelt.

Retningslinjene er supplert med en ny § 3 (b) som anerkjenner at det er en potensiell konflikt mellom personvern og andre grunnleggende rettigheter som følge av den omfattende behandlingen av personopplysninger. Dette er også i samsvar med *Communiqué on Principles for Internet Policy Making*[16] som understreker at ”regler om personvern må balanseres med grunnleggende rettigheter for andre borgere, blant annet ytringsfrihet, trykkefrihet og en åpen og transparent forvaltning”.

De tidligere §§ 15 og 16 i retningslinjene av 1980 er fjernet for å gi større klarhet og unngå gjentakelser, siden medlemslandenes forpliktelse til å sikre global fri flyt av opplysninger og sikkerhet allerede er poengtert andre steder i anbefalingen.

[1] Uttalelse fra dommer Michael Kirby under 30-årsjubileet for OECDs retningslinjer for personvern, http://www.oecd.org/internet/interneteconomy/49710223.pdf.

[2] BCR-systemet er under videreutvikling, se http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm

[3] Se http://www.huntonfiles.com/files/webupload/CIPL_Galway_Conference_Summary.pdf.

[4] APEC, APEC Cross-border Privacy Rules System – Policies, rules and guidelines, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelin

[5] OECD (2007), Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, http://www.oecd.org/internet/interneteconomy/38770483.pdf.

[6] OECD (2011), Council Recommendation on Principles for Internet Policy Making www.oecd.org/internet/interneteconomy/49258588.pdf.

[7] OECD (2011), Communiqué on Principles for Internet Policy Making www.oecd.org/internet/interneteconomy/49258588.pdf.

[8] OECD (2011), "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", *OECD Digital Economy Papers*, No.176, http://dx.doi.org/10.1787/5kgf09z90c31-en.

[9] OECD (2011), "Report on the Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy", *OECD Digital Economy Papers*, No. 178, http://dx.doi.org/10.1787/5kgdpm9wg9xs-en.

[10] OECD (2011), "Terms of Reference for the Review of the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data," http://www.oecd.org/sti/interneteconomy/48975226.pdf

[11] OECD (2012), Recommendation of the Council on Regulatory Policy and Governance, www.oecd.org/gov/regulatorypolicy/49990817.pdf.

[12] *F.eks.* OECD (2002), Guidelines for the Security of Information Systems and Networks: Towards A Culture Of Security, www.oecd.org/internet/interneteconomy/15582260.pdf; OECD (2012), Recommendation of the Council on the Protection of Children Online, http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=272&InstrumentPID=277&Lang=en&Book=False.

[13] G8 (2011), Deauville Declaration: Internet, www.g8.utoronto.ca/summit/2011deauville/2011-internet-en.html.

[14] Kommisjonsavgjørelse 2000/520/EC av 26. juli 2000, iht. direktiv 95/46/EC fra Europaparlamentet og Rådet om i hvor stor grad "safe harbour"-prinsippene er tilstrekkelig for personvernet, samt ofte stilte spørsmål i denne forbindelse, utgitt av US Department of Commerce, Official Journal of the European Communities, 25 August 2000, L-215, 7-47. Se også www.export.gov/safeharbor.

[15] Se OECD (2011), "Report on the Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy", OECD Digital Economy Papers, No. 178, http://dx.doi.org/10.1787/5kgdpm9wg9xs-en.

[16] OECD (2011), Council Recommendation on Principles for Internet Policy Making www.oecd.org/internet/interneteconomy/49258588.pdf.

Utgitt av:
Kommunal- og moderniseringsdepartementet

Opprinnelig publisert av OECD på engelsk og fransk under titlene:
OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data/Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel.
Revidert av OECD i 2013.

Forsidebilde: Eric Fischer - World travel and communication recorded on Twitter. Brukt i hht. CC BY 2.0

Omslagsdesign: DSS - 01/2014