Så stärker vi den personliga integriteten

Slutbetänkande av Integritetskommittén

Stockholm 2017

STATENS OFFENTLIGA UTREDNINGAR

SOU 2017:52

SOU och Ds kan köpas från Wolters Kluwers kundservice.
Beställningsadress: Wolters Kluwers kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@wolterskluwer.se
Webbplats: wolterskluwer.se/offentligapublikationer

För remissutsändningar av SOU och Ds svarar Wolters Kluwer Sverige AB
på uppdrag av Regeringskanslietsförvaltningsavdelning.
Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
En kort handledning för dem som ska svara på remiss.
Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remisser

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck: Elanders Sverige AB, Stockholm 2017

ISBN 978-91-38-24629-0
ISSN 0375-250X

Till statsrådet Morgan Johansson

Regeringen beslutade den 8 maj 2014 att tillkalla en parlamentarisk kommitté med uppdrag att utifrån ett individperspektiv kartlägga och analysera sådana faktiska och potentiella risker för intrång i den personliga integriteten, som kan uppkomma i samband med användning av informationsteknik i såväl privat som offentlig verksamhet (dir. 2014:65).

Regeringen förordnade Göran Gräslund som ordförande. Sist i detta missiv finns en förteckning över förordnade ledamöter i kommittén, experter och sekreterare.

Kommittén antog namnet Integritetskommittén.

Den 18 februari 2016 beslutade regeringen i tilläggsdirektiv till kommittén (dir. 2016:12) att en del av uppdraget skulle redovisas i ett delbetänkande senast den 31 maj 2016. Delbetänkandet skulle enligt beslutet omfatta dels kartläggningen och analysen av riskerna för integritetsintrång, dels ett övervägande om behovet av ett integritetsskyddsråd. Integritetskommittén överlämnade delbetänkandet *Hur står det till med den personliga integriteten?* (SOU 2016:41) den 7 juni 2016.

Kommittén har i det fortsatta arbetet följt upp effekterna i lagstiftningsarbetet av den förstärkning av grundlagsskyddet för den personliga integriteten, som genomfördes år 2011. Kommittén presenterar i slutbetänkandet också förslag på åtgärder för att minska de integritetsrisker som kartlagts.

Stockholm den 7 juni 2017

Göran Gräslund

Agneta Börjesson

Mats Green

Krister Hammarbergh

Ulf Isaksson

Eva-Lena Jansson

Mathias Leveborn

Veronica Lindholm

Elin Lundgren

Jonas Millard

Jessika Roswall

Anders Schröder

Tuve Skånberg

Hanna Wagenius

Heidi-Maria Wallinder

Emanuel Öz

/Maria Jacobsson
Erik Janzon

Förteckning över ledamöter, experter och sekreterare som deltagit i utredningsarbetet samt tider för dessas förordnanden och anställningar

Ledamöter

Göran Gräslund (f.d. generaldirektör, ordförande), fr.o.m. 2014-05-18
Phia Andersson (riksdagsledamot, S), fr.o.m. 2014-06-27 t.o.m. 2015-01-21
Agneta Börjesson (riksdagsledamot, MP), fr.o.m. 2015-05-19
Christoffer Dulny (politisk sekreterare, SD), fr.o.m. 2014-06-27 t.o.m. 2014-10-19
Maria Ferm (riksdagsledamot, MP), fr.o.m. 2014-06-27 t.o.m. 2016-11-06
Xamuel Gonzalez Westling (kommunfullmäktigledamot V), fr.o.m. 2015-04-28 t.o.m. 2016-03-15
Mats Green (riksdagsledamot, M) fr.o.m. 2016-10-20
Krister Hammarbergh (riksdagsledamot, M), fr.o.m. 2014-06-27
Ulf Isaksson (advokat, L), fr.o.m. 2014-06-27
Eva-Lena Jansson (riksdagsledamot, S), fr.o.m. 2015-01-22
Frida Johansson Metso (leg. psykolog, L), fr.o.m. 2014-07-30 t.o.m. 2016-10-17
Ulrika Karlsson (riksdagsledamot, M), fr.o.m. 2014-06-27 t.o.m. 2016-10-19
Mathias Leveborn (kommunikationsansvarig, V), fr.o.m. 2016-03-16
Johan Linander (f.d. riksdagsledamot, C), fr.o.m. 2014-06-27 t.o.m. 2016-03-22
Veronica Lindholm (riksdagsledamot, S), fr.o.m. 2014-10-23
Elin Lundgren (riksdagsledamot, S), fr.o.m. 2014-06-27
Jonas Millard (riksdagsledamot, SD), fr.o.m. 2014-10-20
Andreas Norlén (riksdagsledamot, M), fr.o.m. 2014-06-27 t.o.m. 2016-10-19
Jessika Roswall (riksdagsledamot, M), fr.o.m. 2016-10-20
Anders Schröder (riksdagsledamot, MP), fr.o.m. 2016-11-07
Ardalan Shekarabi (riksdagsledamot, S), fr.o.m. 2014-06-27 t.o.m. 2014-10-22
Tuve Skånberg (riksdagsledamot, KD), fr.o.m. 2014-06-27

Mathias Sundin (riksdagsledamot, L), fr.o.m. 2016-10-18 t.o.m. 2017-04-26
Hanna Wagenius (jurist, C), fr.o.m. 2016-03-23
Heidi-Maria Wallinder (ämneslärare, V), fr.o.m. 2015-05-19
Alice Åström (f.d. riksdagsledamot, V), fr.o.m. 2014-06-27 t.o.m. 2015-04-27
Emanuel Öz (riksdagsledamot, S), fr.o.m. 2015-05-19

Experter

Sara Ahmed, (rättssakkunnig, Justitiedepartementet), fr.o.m. 2016-07-14
Ingela Alverfors (jurist, Datainspektionen), fr.o.m. 2014-08-18 t.o.m. 2015-08-19
Mikael Ejner, (it-säkerhetsspecialist, Post- och telestyrelsen), fr.o.m. 2016-08-25
Fia Ewald (enhetschef, Myndigheten för samhällsskydd och beredskap), fr.o.m. 2014-06-27 t.o.m. 2016-03-22
Anne-Marie Eklund Löwinder (säkerhetschef, Internetstiftelsen i Sverige), fr.o.m. 2014-10-20
Ulrika Harnesk (jurist, Datainspektionen), fr.o.m. 2015-08-20 t.o.m. 2016-09-11
Jens Henriksson, (internationell sekreterare, Sveriges konsumenter), fr.o.m. 2016-07-14
Anna Hörnlund (jurist, Datainspektionen), fr.o.m. 2014-06-27 t.o.m. 2014-08-17
Gunnar Idesten (it-säkerhetsspecialist, Myndigheten för samhällsskydd och beredskap), fr.o.m. 2016-03-23
Jeanette Kronwall (jurist, Post- och telestyrelsen), fr.o.m. 2014-10-20 t.o.m. 2016-07-13
Agneta Runmarker, (dataråd, Datainspektionen) fr.o.m. 2016-09-12
Mårten Schultz (professor, Stockholms universitet), fr.o.m. 2014-06-27

Mathias Säfsten (ämnesråd, Justitiedepartementet),
fr.o.m. 2014-06-27 t.o.m. 2016-07-13

Sekreterare

Maria Jacobsson, jurist, fr.o.m. 2015-11-16
Erik Janzon, enhetschef, fr.o.m. 2014-06-09 t.o.m. 2017-05-31
Katarina Monfils Gustafsson, dåvarande hovrättsassessor, fr.o.m.
2014-07-01 t.o.m. 2015-11-18

Innehåll

DEL IV, Bilagor

Bilagor

DEL I

Inledning

Sammanfattning

Inledning

Vi lever våra liv såväl på nätet, som i den fysiska världen. När vi agerar på nätet lämnar vi spår efter oss. Spår, som går att använda för att underlätta vår vardag, men också för att tjäna pengar på oss och för olika former av kartläggning och övervakning. Det blir allt svårare att ha kontroll på hur våra uppgifter samlas in och vidareanvänds. Integritetskommitténs generella slutsats är att vi som enskilda individer på ett flertal områden drabbas av stegvisa försämringar av den personliga integriteten.

Integritetskommitténs målsättning

Målsättningen för vårt arbete i kommittén har varit att skyddet av den personliga integriteten ska stärkas så att denna grundläggande rättighet är i balans med andra grundläggande rättigheter och legitima samhällsintressen.

Dataskyddsförordningen

Dataskyddsförordningen[1] ska börja tillämpas den 25 maj 2018. Personuppgiftslagen kommer då att upphöra att gälla och en mängd lagar och andra regler kommer att ha anpassats till att vi har en direktverkande EU-lagstiftning i stället.

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

För att bryta den utveckling som innebär stegvisa försämringar av den personliga integriteten behövs en kraftsamling inom en rad områden. Tidpunkten för en sådan kraftsamling är just nu mycket lämplig, med tanke på att samtliga samhällsområden för närvarande lägger ned betydande insatser för att förverkliga förordningens intentioner.

Utvärdering av grundlagsskyddet

Integritetskommittén anser att det är otillfredsställande att 2 kap. 6 § andra stycket regeringsformen tillämpas på så olika sätt av utredningar, myndigheter och inom Regeringskansliet.

En mer enhetlig förståelse och tillämpning av bestämmelsen skulle enligt vår bedömning gynna såväl integritetsskyddet som digitaliseringen av förvaltningen, genom att det tydligare skulle framgå vilka avvägningar som ett förslag aktualiserar. Lagstiftningsarbetet skulle inte på samma sätt som i dag riskera att tappa tempo på grund av att beredningsunderlag behöver kompletteras relativt sent i lagstiftningsprocessen – vilket ibland överhuvudtaget inte låter sig göras. En mer enhetlig förståelse och tillämpning av bestämmelsen skulle också spara resurser i lagstiftningsprocessen.

Vi anser att det är angeläget att statliga kommittéer och särskilda utredare blir bättre på att uppmärksamma och tillämpa det grundlagsfästa kravet på lagstiftningsarbetet som stadgas i 2 kap. 6 § andra stycket regeringsformen. Vi förslår därför att regeringen bör införa en bestämmelse i kommittéförordningen med innebörden att, om ett förslag har betydelse för den personliga integriteten i de fall som avses i 2 kap. 6 § andra stycket regeringsformen, så ska dessa konsekvenser beskrivas i betänkandet.

Integritetskommittén anser också att regeringen bör utvärdera, utveckla och vid behov uppdatera Datainspektionens vägledning för integritetsanalys.

Informationssäkerhet

Vi har som enskilda personer ofta små möjligheter att påverka hur uppgifter om oss hanteras. Vi är hänvisade till att lita på att de personuppgiftsansvariga skyddar uppgifterna. Om uppgifter sprids utan kontroll, försvanskas eller förstörs kan det innebära integritetskränkningar. Brister i informationssäkerhet medför alltså ett sämre skydd för den personliga integriteten.

Vi konstaterar att det pågår flera olika utredningar och satsningar i Sverige och på EU-nivå som syftar till att förbättra informationssäkerheten i samhället. Dataskyddsförordningen kommer också att ställa krav på de personuppgiftsansvariga och personuppgiftsbiträdena avseende såväl tekniska som organisatoriska informationssäkerhetsåtgärder. Men även Integritetskommittén lämnar ett par förslag på detta område.

Vissa av de skyddsåtgärder som kan användas, exempelvis anonymisering, pseudonymisering och kryptering, är svåra att införa inom vissa samhällssektorer. Därför finns det ett behov av samordning på nationell nivå, exempelvis när det gäller standarder och normer. Det finns även ett behov av att i högre grad integrera arbetet med att skydda den personliga integriteten med det traditionella informationssäkerhetsarbetet.

Kommittén anser också att det finns ett behov av mer och bättre tillsyn över statliga myndigheters informationssäkerhet.

Vi anser därför att regeringen bör bereda ett redan befintligt förslag om att Myndigheten för samhällsskydd och beredskap (MSB) ska utöva tillsyn över den statliga sektorns informationssäkerhet.

I kapitel 12 om informationssäkerhet beskriver vi våra förslag på detta område.

Integritetsstärkande arbete

Det pågår en rad olika utredningar och satsningar i Sverige och på EU-nivå som syftar till att förbättra integritetsskyddet.

Flera statliga utredningar har arbetat och arbetar med att anpassa vår lagstiftning till dataskyddsförordningen. Dataskyddsutredning-

en[2] har föreslagit[3] de anpassningar och kompletterande författningsbestämmelser på generell nivå, som förordningen ger anledning till. Syftet är att säkerställa att det finns en ändamålsenlig och välbalanserad kompletterande nationell reglering om personuppgiftsbehandling på plats, när förordningen börjar tilllämpas. Forskningsdatautredningen[4] ska i sin tur bland annat analysera vilken reglering av personuppgiftsbehandling för forskningsändamål som är möjlig och kan behövas utöver den generella reglering, som Dataskyddsutredningen har föreslagit med anledning av förordningen.

Den omständigheten att dataskyddsförordningen ska börja tilllämpas om mindre än ett år ger en särskild skjuts åt arbetet med att stärka integritetsskyddet. Samtliga personuppgiftsansvariga måste arbeta med att anpassa sin personuppgiftshantering till de nya bestämmelserna.

Vidare har man i Regeringskansliet arbetat med att ta fram en nationell strategi för informations- och cybersäkerhet, som tar sin utgångspunkt i det förslag som lades fram i betänkandet *Informations- och cybersäkerhet i Sverige*.[5] Strategin ska presenteras under sommaren 2017.

Utredningen om genomförande av NIS-direktivet har haft i uppdrag att föreslå hur EU-direktivet om åtgärder för en hög gemensam nivå av säkerhet i nätverk och informationssystem ska genomföras i svensk rätt.[6] Utredaren föreslår i betänkandet *Informationssäkerhet för samhällsviktiga och digitala tjänster*[7] bland annat hur direktivets krav på utpekande av myndigheter med ansvar för vissa funktioner ska genomföras. Inriktningen är att MSB ska ges en samordnande roll på området, men att andra myndigheters ansvar för tillsyn inom särskilda sektorer ska fortsätta att gälla.

[2] Dir. 2016:15.
[3] Dataskyddsutredningens betänkande *Ny dataskyddslag* (SOU 2017:19).
[4] Dir. 2016:65 och dir. 2017:29.
[5] NISU:s 2014 betänkande *Informations- och cybersäkerhet i Sverige*, (SOU 2015:23).
[6] Europaparlamentets och Rådets direktiv (eu) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.
[7] SOU 2017:36.

Integritetskommitténs övriga förslag till åtgärder

Vårt huvuduppdrag har varit att från ett individperspektiv kartlägga och analysera faktiska och potentiella risker för intrång i den personliga integriteten i samband med användning av informationsteknik. Denna granskning presenterade vi i vårt delbetänkande *Hur står det till med den personliga integriteten?* [8] Vi har sett det som vårt uppdrag att också ge förslag på åtgärder som kan stärka skyddet för den personliga integriteten.

I detta betänkande presenteras förslagen utifrån olika verksamhetsområden som behandlar uppgifter om oss som enskilda. Här sammanfattar vi några av de viktigaste förslagen.

Uppförandekoder

Sammanslutningar, som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden, kan inom en viss bransch eller sektor lämna förslag till specificeringar om hur man i praktiken ska tillämpa dataskyddsförordningen inom sitt område. Sådana specificeringar kallas i dataskyddsförordningen för uppförandekoder. En uppförandekod kan även omfatta verksamhet som bedrivs av myndigheter. En uppförandekod kan också beskrivas som en sorts branschvis självreglering i syfte att konkretisera regelverket. Vi tror att uppförandekoder kan bli ett effektivt hjälpmedel för att höja skyddet av den personliga integriteten inom flera områden.

Arbetet med att ta fram förslag till uppförandekoder ska utföras av de personuppgiftsansvarigas eller personuppgiftsbiträdenas branschorganisationer, men arbetet med att uppmuntra, granska och godkänna uppförandekoder är enligt dataskyddsförordningen ett uppdrag för myndigheter.

Vi föreslår t.ex. att regeringen uppdrar åt Konsumentverket att initiera och stödja utarbetandet av uppförandekoder för branscher där personuppgifter hanteras för huvudsakligen kommersiella ändamål. Integritetskommittén bedömer att uppdraget i första hand ska inriktas mot att specificera tillämpningen rörande samtycke respektive intresseavvägning som laglig grund för behandlingen av person-

[8] Integritetskommitténs delbetänkande *Hur står det till med den personliga integriteten?* (SOU 2016:41).

uppgifter, samt innehåll och form för den information som ska ges till de registrerade. I arbetet med att initiera och stödja framtagandet av uppförandekoder, kan Konsumentverket exempelvis bjuda in branschorganisationerna och andra ansvariga myndigheter till ett samtal om förutsättningarna för en uppförandekod på området (kapitel 9).

Vi föreslår också att Skolverket ges i uppdrag att initiera och stödja utarbetandet av en uppförandekod för hantering av personuppgifter i skolan (kapitel 5).

När det gäller hantering av personuppgifter i hälso- och sjukvården och socialtjänsten föreslår vi också att en myndighet får i uppdrag att initiera och stödja utarbetandet av en uppförandekod. För att ytterligare stödja de personuppgiftsansvariga i denna känsliga personuppgiftshantering föreslår vi därtill att den myndighet som får uppdraget, ska upprätta ett sekretariat som stödjer de personuppgiftsansvariga i det praktiska arbetet med koden (kapitel 7).

Tydligare reglering i lag

Inom vissa områden har Integritetskommittén konstaterat att det saknas viktig reglering om hur personuppgifter ska hanteras. Denna brist lämnar de personuppgiftsansvariga i ett svårt läge. De har ansvaret för att på bästa sätt tolka den allmänt hållna reglering som finns, men riskerar att trots god vilja göra fel bedömningar, vilket naturligtvis i slutändan också riskerar att drabba den enskilde.

Vi har inte haft möjlighet att inom ramen för vårt uppdrag ta fram kompletta lagförslag. Vi föreslår därför ytterligare utredningar eller beredningar av tidigare lagda lagförslag inom flera områden, bland annat dessa:

En ny socialtjänstdatalag

Integritetskommittén anser att det behövs en ny reglering för den personuppgiftsbehandling som förekommer inom socialtjänsten. Personuppgiftsbehandlingen inom socialtjänsten bör i likhet med personuppgiftsbehandlingen i hälso- och sjukvården regleras i en egen lag. En sådan lag bör utformas med beaktande av det lagstiftningsutrymme som dataskyddsförordningen ger. En komplett och tydlig

lagstiftning inom detta område ökar förutsättningarna för ett ordnat införande av välfärdsteknik inom socialtjänsten. Regeringen bör, med utgångspunkt i befintliga förslag, utreda möjligheten till ny lagstiftning som reglerar hantering av personuppgifter inom socialtjänsten och som kompletterar och specificerar kraven i dataskyddsförordningen (kapitel 7).

Nya integritetsstärkande regler bör skyndsamt införas i patientdatalagen

Vårdgivarens övergripande ansvar för en säker och ändamålsenlig hantering av personuppgifter i verksamheten bör uttryckas tydligare och på ett samlat sätt i patientdatalagen. Vi anser att det behövs ett kapitel i lagen som samlar de bestämmelser som förtydligar både vårdgivarens och hälso- och sjukvårdspersonalens ansvar för en säker hantering av personuppgifter i verksamheten. Regler som ökar detaljeringsnivån i lagen kan göra det lättare för de verksamheter som ska tillämpa regelverket (kapitel 7).

En reglering av medborgarprofilering

I delbetänkandet konstaterade Integritetskommittén att det finns allvarliga risker för den personliga integriteten i sådan kontrollverksamhet hos myndigheter, som syftar till att i förväg bedöma vilken sannolikhet det finns för att en viss individ ska begå någon form av felaktighet. Denna typ av kontroller kallas ibland för ”smarta kontroller” eller ”urvalsprofiler”. I delbetänkandet använde vi uttrycket ”medborgarprofilering” som samlingsbegrepp för företeelsen. Vi anser att det finns ett behov av att kartlägga hur både statliga och kommunala myndigheter arbetar med smarta kontroller och att föreslå de lagändringar som behövs för att ge denna verksamhet en tydlig och legal grund och styrning, som beaktar både behovet av kontroller och den enskildes personliga integritet samt rätten att inte bli diskriminerad. Kommittén anser därför att regeringen bör utreda denna fråga närmare (kapitel 8).

Sekretesskydd i skolan

Det genereras allt fler och allt mer detaljerade uppgifter om eleverna i skolan, alltifrån hur de använder sig av läromedel och chattar med klasskamraterna, till vilka kamrater de helst syns tillsammans med i skolan. För elever i grundskolan och gymnasieskolan finns inte någon sekretess eller tystnadsplikt för större delen av den växande uppgiftsmassan. Vi anser att regeringen bör utreda frågan om ett utökat sekretsskydd för uppgifter om elever i skolans it-system (kapitel 5).

Lagreglering av vissa spaningsmetoder

När det gäller de brottsbekämpande myndigheternas verksamhet har vi gjort bedömningen att det finns påtagliga risker för den personliga integriteten när det gäller vissa integritetskänsliga spaningsmetoder. Det gäller t.ex. användning av dolda kroppsmikrofoner, handmanövrerade kameror, kopiering av mobiltelefoner och datorer och pejling. Även användningen av falska basstationer och installation av spionprogram är exempel på sådana spaningsmetoder. Vi anser därför att regeringen bör utreda en lagreglering av sådana integritetskänsliga spaningsmetoder som i dag inte är reglerade eller har svag reglering (kapitel 11).

Anslag till tvärvetenskaplig forskning om digitalisering och personlig integritet

Vi har konstaterat att det finns förhållandevis lite forskning om vilken inverkan den digitala utvecklingen har på människan och hennes uppfattning om världen och om sig själv. Forskning om digitalisering och personlig integritet är ett område som förtjänar större uppmärksamhet; både för att höja kunskapsnivån men också för att bidra till att finna lösningar av tekniska och legala utmaningar. Vi föreslår därför att regeringen ger Vetenskapsrådet i uppdrag att fördela anslag till tvärvetenskaplig forskning om frågan på vilket sätt människan påverkas av förändringar i den privata sfären och av den accelererande digitala hanteringen av personuppgifter.

Kompetenscenter för frågor som rör anskaffning och användning av externa it-tjänster.

Integritetskommittén har uppmärksammat risker till följd av brister i myndigheternas kompetens när det gäller it-utveckling. Ett kompetenscenter skulle kunna bidra till att den offentliga förvaltningen blir bättre kravställare i upphandlingar, bland annat vad gäller kraven på inbyggd integritet och informationssäkerhet. Bättre och tydligare krav från det allmännas sida kan även påverka marknaden utanför offentlig sektor. Vi anser därför att regeringen bör uppdra åt den myndighet som får det samlade ansvaret för den offentliga förvaltningens digitalisering att inrätta ett kompetenscenter för frågor som rör anskaffning och användning av externa it-tjänster.

Statskontoret bör få i uppdrag att utföra en myndighetsanalys av Datainspektionen

Vi anser att tillsynen över de personuppgiftsansvariga och personuppgiftsbiträdena är mycket viktig. Genom tillsynen agerar staten för att skydda oss mot olaglig hantering av våra personuppgifter. Nya sätt att behandla våra uppgifter introduceras i en mycket snabb takt. Många av dessa finns det anledning att bedöma ur ett rättsligt perspektiv. Regelverket är tämligen oprecist och allmänt hållet. Det är därför ofta först när tillsynsmyndigheten har bedömt en ny företeelse som leverantörer och användare får någon ledning. Resultatet från tillsynen kan sedan användas i tillsynsmyndighetens utåtriktade och proaktiva arbete för att sprida kunskap. I delbetänkandet konstaterade vi dock att Datainspektionen på senare år successivt har minskat sina tillsynsaktiviteter.

I delbetänkandet konstaterade kommittén att flera myndigheter efterlyser mer vägledning från tillsynsmyndigheten i samband med digitaliseringen av förvaltningen. Även i flera av remissvaren på vårt delbetänkande framförs önskemål om tydligare och mer konkret vägledning från Datainspektionen i frågor som rör integritetsskydd.

Datainspektionen kommer på grund av dataskyddsförordningen att få många nya arbetsuppgifter och kommer även att behöva samverka mer både nationellt och internationellt. Detta samtidigt som de personuppgiftsansvariga i och med den nya förordningen kommer att behöva mycket mer stöd och vägledning. Parallellt med den-

na utveckling kommer Datainspektionen, på samma sätt som alla andra myndigheter, att behöva utveckla och förbättra sin verksamhet och sina arbetssätt.

För att klargöra vilket anslag, vilka resurser och vilka kompetenser, som Datainspektionen behöver de närmaste åren, anser Integritetskommittén att regeringen bör ge Statskontoret i uppdrag att utföra en myndighetsanalys av Datainspektionen enligt den modell som Statskontoret redovisade till regeringen i december 2008 i rapporten *Modell för myndighetsanalyser* (2008:17).

Den myndighet, som får det samlade ansvaret för den offentliga förvaltningens digitalisering, bör även främja skyddet av den personliga integriteten

Integritetskommittén anser att det är av största betydelse att den myndighet som får det samlade ansvaret för digitaliseringen av offentlig sektor, även får i uppgift att beakta skyddet för den personliga integriteten. I instruktionen för den myndigheten bör det därför anges att denna myndighet ska främja skyddet av den personliga integriteten, med särskilt fokus på införandet av integritetsskyddande teknik och arbetssätt. Myndigheten måste förstås samverka med Datainspektionen i detta arbete.

Konsekvenser av våra förslag

Dataskyddsförordningen ska börja tillämpas i Sverige. Alternativet till våra genomgripande förslag om att arbeta med uppförandekoder, är således inte att myndigheter och företag avstår från att vidta åtgärder eller genomföra förändringsarbete, utan snarare att företag, myndigheter och andra organisationer tvingas lägga mer resurser på att tolka rättsläget.

Vi menar att flera av våra förslag kommer att innebära minskade kostnader för både företag och myndigheter (såväl statliga som kommunala). Konsekvensanalysen finns i kapitel 17.

Hela listan med Integritetskommitténs bedömningar och förslag

Skolan (kap. 5)

1. Regeringen bör ge Skolverket i uppdrag att initiera och stödja utarbetandet av en uppförandekod för skolan.
2. Regeringen bör låta utreda ett utökat sekretesskydd för uppgifter om elever i skolans it-system.
3. Regeringen bör ge Skolinspektionen och Datainspektionen i uppdrag att hitta lämpliga samarbetsformer.

Arbetslivet (kap. 6)

4. Regeringen bör ge Arbetsmiljöverket i uppdrag att initiera och stödja utarbetandet av uppförandekoder inom arbetslivet.

Hälso- och sjukvård och välfärdsteknik inom socialtjänsten (kap. 7)

5. Regeringen bör ge en myndighet, förslagsvis E-hälsomyndigheten, i uppdrag att initiera och stödja utarbetandet av uppförandekoder inom hälso- och sjukvård och socialtjänst.
6. Regeringen bör ge en myndighet, förslagsvis E-hälsomyndigheten, i uppdrag att vara sekretariat för förvaltningen av de gemensamma uppförandekoderna.
7. Regeringen bör vidta de utredningsåtgärder som är nödvändiga för att genomföra de lagändringar, som tidigare utredningar föreslagit i syfte att stärka integriteten vid behandling av personuppgifter.
8. Regeringen bör låta utreda en ny lagstiftning om personuppgiftshantering inom socialtjänsten.
9. Det behövs lagregler om ställföreträdare för beslutsoförmögna.

E-förvaltning (kap. 8)

10. I instruktionen för den myndighet som får det samlade ansvaret för den offentliga förvaltningens digitalisering, bör anges att denna myndighet även ska främja skyddet av den personliga integriteten, och särskilt stödja lösningar som nyttjar integritetsskyddande arbetssätt och teknik.
11. Regeringen bör ge samma myndighet i uppdrag att inrätta ett kompetenscenter för frågor som rör anskaffning och användning av externa it-tjänster.
12. Regeringen bör låta utreda hur ett regelverk för tystnadsplikt för leverantörer av molntjänster och andra personuppgiftsbiträden skulle kunna utformas.
13. Integritetskommittén ställer sig bakom förslaget från Statens servicecenter att regeringen i närtid bör initiera ett uppdrag att närmare analysera förutsättningarna för att inrätta en ”statens molntjänst” i enlighet med rapporten från Statens servicecenter.
14. Regeringen bör låta utreda hur statliga och kommunala myndigheter arbetar med medborgarprofilering (även kallat ”smarta kontroller”), hur myndigheterna bör eller kan arbeta med sådana kontroller, samt föreslå de lagändringar som behövs.
15. Regeringens digitala strategier bör kompletteras med ett inriktningsmål med den uttryckliga ambitionen att Sverige ska bli världsledande både när det gäller att använda digitaliseringens möjligheter och att skydda den personliga integriteten.

Konsumentområdet (kap. 9)

16. Regeringen bör ge i uppdrag till Konsumentverket att initiera och stödja utarbetandet av uppförandekoder för branscher där personuppgifter hanteras för huvudsakligen kommersiella ändamål.
17. Regeringen bör ge i uppdrag till Konsumentverket att utöva tillsyn över företeelser, produkter och avtal där integritetsskydd och informationssäkerhet gör sig gällande.

Försäkringsverksamhet (kap. 10)

18. Konsumentverket bör bevaka försäkringsföretagens arbete med uppförandekoder.

19. Regeringen bör vidta de utredningsåtgärder som är nödvändiga för att genomföra en lagreglerad tystnadsplikt för försäkringsföretagen och deras anställda avseende personuppgifter.

Åtgärder inom några andra områden med allvarliga eller påtagliga risker (kap. 11)

20. Regeringen bör låta utreda hur en säker ordning för utfärdande av fysiska legitimationer ska se ut och hur statens ansvar för den ska vara utformad.

21. Regeringen bör låta utreda en författningsreglerad rättighet för fysiska personer att vända sig till den som ger ut en kreditupplysningspublikation för att (inom ramen för vad som är förenligt med grundlagarna) få uppgifter om sig själv strukna innan uppgifterna publiceras.

22. Det är angeläget att regeringen lämnar förslag på reglering som ger integritetsskydd vid utlämnande av kreditupplysning, oavsett hur kreditupplysningen lämnas ut. Detta kan göras med utgångspunkt i förslag som redan föreligger.

23. Regeringen bör låta utreda en lagreglering av sådana integritetskänsliga spaningsmetoder inom polisen som i dag inte är reglerade eller har svag reglering.

Informationssäkerhet (kap. 12)

24. Regeringen bör vidta de utredningsåtgärder som är nödvändiga för att genomföra det förslag som lämnades i SOU 2015:23 om att MSB ska utöva tillsyn över statliga myndigheters informationssäkerhetsarbete.

25. Regeringen bör uppdra åt MSB att beträffande myndigheter under regeringen följa upp vilka åtgärder myndigheterna vidtar

för att följa kraven i MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1).

26. De insatser för att åstadkomma uppförandekoder som kommittén föreslår i andra avsnitt i detta betänkande, bör innehålla informationssäkerhetsåtgärder som framträdande inslag. Om insatserna förverkligas, kan de innebära en generell förbättring av förutsättningarna för en bättre informationssäkerhet i samhället.

27. Regeringen bör ge MSB i uppdrag att i samverkan med andra myndigheter utveckla, förvalta och vidareutveckla en styrmodell för statens informationssäkerhet, i enlighet med det som föreslagits i SOU 2015:23.

Samhällets skyddsmekanismer (kap. 13)

28. Regeringen bör låta utreda om Datainspektionen ska ges rätten att som part föra talan i domstol för enskilda i utvalda ersättningsärenden.

29. Datainspektionen bör ges i uppdrag att årligen rapportera till regeringen om rättsmedlen är effektiva för att skydda registrerades rättigheter.

30. Regeringen bör följa upp att Riksrevisionens rekommendationer följs avseende kompetens och metod för utredning av it-relaterad brottslighet och sedan redovisa resultatet för riksdagen.

31. Regeringen bör ge en myndighet i uppdrag att utreda hur en nationell folkbildningsinsats bör vara organiserad och utformad samt vilken omfattning och finansiering en sådan insats bör ha.

Tillsynsmyndigheten (kap. 14)

32. Regeringen bör ge Statskontoret i uppdrag att utföra en myndighetsanalys av Datainspektionen enligt den modell som Statskontoret redovisade till regeringen i december 2008 i rapporten *Modell för myndighetsanalyser* (2008:17).

Forskning om personlig integritet (kap. 15)

33. Regeringen bör ge Vetenskapsrådet i uppdrag att fördela ett särskilt forskningsanslag.

34. Regeringen bör ge Vinnova i uppdrag att främja projekt som involverar integritetsskyddande teknik och arbetssätt samt att upplysa om och kravställa utifrån dataskyddsförordningen i sitt arbete.

Utvärdering av grundlagsskyddet (kap. 16)

35. Regeringen bör i kommittéförordningen (1998:1474) införa en bestämmelse som föreskriver att om förslagen i ett betänkande har betydelse för den personliga integriteten i de fall som avses i 2 kap. 6 § andra stycket regeringsformen, ska konsekvenserna i det avseendet anges i betänkandet.

36. Regeringen bör utvärdera, utveckla och vid behov uppdatera den av Datainspektionen utgivna vägledningen för integritetsanalys.

Summary

Introduction

We live our lives both online and in the physical world. When we are on the internet we leave traces behind. These traces can be used to make our everyday lives easier, but also to make money from us and to conduct various forms of tracking and monitoring. It is becoming increasingly difficult to maintain control of how data is collected and re-used. The Privacy Committee's general conclusion is that we, as private individuals, are being affected in a number of areas by a gradual deterioration of our privacy.

The Privacy Committee's objective

The objective for our work in the Committee was to ensure that protection of privacy is strengthened so that this fundamental right is balanced with other fundamental rights and legitimate societal interests.

The General Data Protection Regulation

The General Data Protection Regulation[1] will begin to apply on 25 May 2018. The Personal Data Act will then cease to apply and a number of acts and other rules will have been adapted to the fact that we have directly applicable EU legislation instead.

[1] 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

To break the trend of a gradual deterioration of privacy, a concerted effort is needed in a number of areas. The timing of such a concerted effort is very apt right now in view of all of the areas of society that are currently putting a great deal of work into realising the intentions of the Regulation.

Evaluation of constitutional protection

The Privacy Committee considers that it is unsatisfactory that the provision in Chapter 2, Article 6, second paragraph of the Instrument of Government is applied in such different ways by inquiries and government agencies, and within the Government Offices.

In our view, a more consistent understanding and application of the provision would benefit both privacy protection and eGovernment as it would be clearer which considerations a proposal raises. Legislative work would not risk losing momentum, as is currently the case, due to the fact that preparatory material needs to be supplemented relatively late in the legislative process – which is sometimes not even possible. A more consistent understanding and application of the provision would also save resources for the overall work involved in the legislative process.

We consider that it is important that central government committees and inquiry chairs become better at drawing attention to and applying the constitutional requirement for legislative work, as stated in Chapter 2, Article 6, second paragraph of the Instrument of Government. We therefore propose that the Government introduce a provision in the Committees Ordinance stating that if a proposal has a bearing on privacy in the cases referred to in Chapter 2, Article 6, second paragraph of the Instrument of Government, the consequences in this regard must be described in the report.

The Committee also considers that the Government should evaluate, develop and, where necessary, update the Swedish Data Protection Authority's guidance for privacy analyses.

Information security

As private individuals, we often have few possibilities to influence how data about us is processed and we have to rely on personal data controllers to protect our data. If data is spread without any control, distorted or destroyed, this can lead to violations of privacy. Shortcomings in information security therefore result in lesser protection for people's privacy.

We note that there are several different inquiries and initiatives under way in Sweden and at EU level aimed at improving information security in society. The General Data Protection Regulation will also set standards for controllers in terms of both technical and organisational information security measures. But we also present a few proposals in this area.

Some of the protective measures that can be used, such as anonymisation, pseudonymisation and encryption, are difficult to introduce in certain sectors of society. There is therefore a need for coordination at national level, for example in terms of standards and norms. There is also a need to more closely integrate work to protect privacy with traditional information security work.

The Committee also considers that there is a need for more and better supervision of government agencies' information security.

We therefore consider that the Government should look into an existing proposal stating that the Swedish Civil Contingencies Agency should exercise supervision of information security in the state sector.

More proposals in this area are contained in chapter 12 on information security.

Privacy enhancement efforts

A number of different inquiries and initiatives are under way in Sweden and at EU level aimed at improving privacy protection in our society.

Several central government inquiries are working on adapting our legislation to the General Data Protection Regulation. The Data

Protection Inquiry[2] proposes a new national regulation that supplements the General Data Protection Regulation at a general level. However, its work was not intended to broaden or restrict the possibilities of processing personal data, other than in cases where the General Data Protection Regulation requires such a change.[3]

The Research Data Inquiry[4] will, in turn, analyse what regulation of personal data processing for research purposes is possible and may be needed in addition to the general regulations that the Data Protection Inquiry proposes as a result of the Regulation.

The fact that the General Data Protection Regulation will begin to apply in less than one year gives particular momentum to efforts to strengthen privacy protection. All controllers must work on adapting personal data processing to the new provisions.

In addition, the Government Offices has been working on a national strategy for information and cyber security, which is based on the proposal presented in the report entitled 'Information and cyber security in Sweden' (SOU 2015:23). The strategy will be presented in the summer of 2017.

The Privacy Committee's proposals for measures

Our main remit was to identify and analyse, from the individual's perspective, the actual and potential risks of violations of privacy in connection with the use of information technology. We presented this investigation in our interim report entitled 'What is the privacy situation?' [5] We have considered it our remit to also present proposals for measures that can strengthen protection of privacy.

In this final report, we therefore present a number of proposals for measures and assessments. The report presents the proposals on the basis of various areas of activity that process data about us as individuals. Some of the most important proposals are summarised below.

[2] ToR 2016:15.
[3] Report entitled 'Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning' (SOU 2017:39) with a summary in English starting om page 29.
[4] ToR 2016:65 and ToR 2017:29.
[5] Interim report of the Privacy Committee: 'What is the privacy situation?' (SOU 2016:41).

Codes of conduct

Associations and other bodies representing categories of controllers or processors can, in a certain industry or sector, present proposals for specifications on how to apply the General Data Protection Regulation in that area in practice.[6] These kinds of specifications are called 'codes of conduct' in the General Data Protection Regulation. A code of conduct can also cover activities conducted by the public administration. Further, a code of conduct can be described as a kind of sector-specific self-regulation aimed at concretising the regulatory framework. We believe that codes of conduct can be an effective aid to increase the protection of privacy in several areas.

Work to produce codes of conduct should be carried out by controllers' or processors' industry organisations, but under the General Data Protection Regulation, the work to promote, scrutinise and approve codes of conduct is a job for government agencies.

We propose, for example, that the Government task the Swedish Consumer Agency with initiating and supporting the drafting of codes of conduct for industries in which personal data is processed mainly for commercial purposes. The Committee considers that the remit should primarily focus on specifying application of the Regulation in terms of consent or balancing of interests as a legal basis for the processing of personal data, and content and form for the information that will be provided to data subjects. In its work to initiate and support the drafting of codes of conduct, the Swedish Consumer Agency could host consultations with industry organisations and other responsible agencies on the conditions for a code of conduct in that area (chapter 9).

We also propose that the National Agency for Education be tasked with initiating and supporting the drafting of a code of conduct for processing personal data in schools (chapter 5).

With regard to the processing of personal data in health and medical care and social services, we also propose that a government agency be tasked with initiating and supporting the drafting of a code of conduct. To further support controllers in the sensitive work of personal data processing, we also propose that the agency

[6] 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.

given the remit should establish a secretariat to support controllers in the practical work of drafting the code (chapter 7).

Clearer regulations in law

In certain areas, the Committee has noted that important regulation is lacking on how personal data should be processed. This shortcoming puts controllers in a difficult position. They have responsibility for interpreting the general regulation in the best way possible, but despite their good intentions they risk making the wrong assessments, which of course ultimately also risks affecting individuals.

In this area, we have not had the possibility to draft complete legislative proposals ourselves. We therefore propose further inquiries or preparation processes for previously presented legislative proposals in a number of areas, including the following:

A new Social Services Data Act

The Privacy Committee considers that a new regulation is needed for the personal data processing carried out in social services. Personal data processing within social services should be regulated in a separate act, as is the case with personal data processing in health and medical care. This act should be designed to take account of the legislative scope provided by the General Data Protection Regulation. Complete and clear legislation in this area would improve the prospects of the orderly introduction of welfare technology in social services. The Government should, on the basis of existing proposals, look into the possibility of passing new legislation that regulates the processing of personal data in social services and supplements and specifies the requirements of the General Data Protection Regulation (chapter 7).

New privacy-enhancing rules should be swiftly introduced in the Patient Data Act

The overall responsibility of care providers for the secure and appropriate processing of personal data in their activities should be more clearly and coherently expressed in the Patient Data Act. We believe that the Act needs a chapter that brings together the provisions clarifying the responsibility of both care providers and health and medical care staff for the secure processing of personal data in their activities. Rules that increase the level of detail in the Act could make it easier for activities in which the regulatory framework is to be applied (chapter 7).

Regulation of citizen profiling

In its interim report, the Committee noted that there are serious risks for privacy in the kind of control activities conducted by agencies that are intended to assess in advance the probability of a certain individual committing some form of error. These kinds of controls are sometimes called 'smart controls' or 'selection profiles', and in the interim report we used the term 'citizen profiling'.[7] We consider there is a need to identify how both government agencies and local government authorities are using smart controls and to propose the legislative amendments needed to give this activity a clear and legal basis and governance that take account of the need for controls and individual privacy and the right not to be discriminated against. The Committee therefore considers that the Government should look into this issue more closely (chapter 8).

Secrecy protection in schools

Increasing amounts of increasingly detailed data about pupils in schools is being generated – everything from how they use teaching aids and chat forums with their classmates to which friends they prefer to be seen with in school. For pupils in compulsory school and upper secondary school there is no secrecy or duty of confidentiality

[7] In the interim report, we use *citizen profiling* as the umbrella term for these phenomena.

for the majority of this growing mass of data. We consider that the Government should investigate the issue of expanding secrecy protection to cover data about pupils contained in school IT systems (chapter 5).

Regulation in law of certain surveillance methods

Regarding the activities of the law enforcement agencies, we consider that there are tangible risks for privacy concerning surveillance methods that are sensitive in terms of privacy. This applies to the use of concealed body microphones, hand-held cameras, copying of mobile phones and computers, and tracking devices, for example. The use of fake base stations and the installation of spy programmes are also examples of such surveillance methods. We therefore consider that the Government should look into a legislative regulation of such surveillance methods that are sensitive in terms of privacy and that are currently not regulated or that are subject to weak regulation (chapter 11).

Grants for interdisciplinary research on digitalisation and privacy

We have noted that there is relatively little research on the effect of digital developments on people's behaviour and their view of the world and themselves. Research into digitalisation and privacy is an area that deserves greater attention, both to increase the level of knowledge and to help find solutions to technical and legal challenges. We therefore propose that the Government task the Swedish Research Council with distributing grants for interdisciplinary research into the issue of how people and their behaviour are affected by the accelerated digital processing of their data and private spheres.

Centre of excellence for issues concerning the acquisition and use of external IT services

The Committee has drawn attention to the risks associated with shortcomings in agencies' expertise in the area of IT development. A centre of excellence could help public administration become better at setting requirements in procurements, including the requirement for built-in privacy and information security. Better and clearer requirements from the public sector could also have an impact on the market outside the public sector. We therefore consider that the Government should task the agency given overall responsibility for the digitalisation of public administration with establishing a centre of excellence for issues concerning the acquisition and use of external IT services.

The Swedish Agency for Public Management should be tasked with conducting an agency analysis of the Swedish Data Protection Authority

We consider that the supervision of controllers is very important. Through supervision, the State takes action to protect us against the unlawful processing of our personal data. New ways of processing our data are being introduced at a very rapid pace. There is cause to assess many of these from a legal perspective. The regulatory framework is rather imprecise and kept intentionally vague. It is therefore often the case that suppliers and users do not receive any guidance until the supervisory agency has assessed a new phenomenon. The results of this supervision can then be used in the supervisory agency's outreach and proactive work to disseminate knowledge. However, in the interim report we noted that the Swedish Data Protection Authority has gradually reduced its supervisory activities in recent years.

In its interim report, the Committee noted that a number of agencies have requested more guidance from the supervisory agency in connection with eGovernment. In several consultation responses to our interim report, the desire for clearer and more concrete guidance from the Swedish Data Protection Authority is also presented concerning privacy protection issues.

With the new General Data Protection Regulation, the Swedish Data Protection Authority will receive many new tasks and will also need to cooperate more both nationally and internationally. And at the same time, with the new Regulation, society will need much more support and guidance. Parallel to this development, the Swedish Data Protection Authority will – like all other government agencies – need to develop and improve its activities and its working methods.

To clarify which appropriations, which resources and which skills the Swedish Data Protection Authority will need over the coming years, we consider that the Government should task the Swedish Agency for Public Management with conducting an agency analysis of the Swedish Data Protection Authority in line with the model it presented to the Government in December 2008 in the report entitled 'Model for agency analyses' (2008:17).

The agency given overall responsibility for the digitalisation of public administration should also promote protection of privacy

The Privacy Committee believes that it is extremely important that the agency given the overall responsibility for the digitalisation of public administration, is also tasked with safeguarding protection of privacy. The instructions for the agency should therefore state that this agency is to promote protection of privacy, with a special focus on the introduction of privacy enhancing working methods and technologies. Naturally, the agency must work with the Swedish Data Protection Authority on these tasks.

Consequences of our proposals

The General Data Protection Regulation will be implemented in Sweden. The alternative to the our far-reaching proposals on working with codes of conduct is therefore not for agencies and companies to refrain from taking measures or implementing change; instead, companies, agencies and other organisations would be forced to invest more resources in interpreting the legal situation.

We believe that a number of our proposals will entail reduced costs for both companies and agencies (both at central government and local level). The impact assessment is in chapter 17.

Full list of the Privacy Committee's proposals

The School (chapter 5)

1. The Government should instruct the National Agency for Education to take measures to initiate and support the drafting of a code of conduct for schools.
2. The Government should appoint an inquiry into expanded secrecy protection for data about pupils in school IT systems.
3. The Government should task the Swedish Schools Inspectorate and the Swedish Data Protection Authority with finding suitable forms of cooperation.

Working life (chapter 6)

4. The Government should task the Swedish Work Environment Authority with initiating and supporting the drafting of codes of conduct in working life.

Health and medical care and welfare technology in social services (chapter 7)

5. The Government should task an agency, possibly the Swedish eHealth Agency, with initiating and supporting the drafting of codes of conduct in health and medical care and social services.
6. The Government should task an agency, possibly the Swedish eHealth Agency, with acting as a secretariat for the management of the common codes of conduct.
7. The Government should implement legislative amendments aimed at strengthening privacy, as previous inquiries have proposed.
8. The Government should introduce new legislation on personal data processing in social services.
9. The Government should introduce a legal regulation on representatives for people who lack decision-making capacity.

eGovernment (chapter 8)

10. The instructions for the agency given overall responsibility for the digitalisation of public administration should state that this agency must also promote protection of privacy and, in doing so, give particular support to solutions that use privacy enhancing working methods and technologies.
11. The Government should task the same agency with establishing a centre of excellence for issues concerning the acquisition and use of external IT services.
12. The Government should look into the duty of confidentiality for suppliers of cloud services and other personal data processors.
13. The Privacy Committee supports the proposal from the National Government Service Centre that the Government should, in the near future, initiate a remit to closely analyse the conditions for establishing a 'state cloud service' in line with the report from the National Government Service Centre.
14. The Government should look into how government agencies and local government authorities are working on citizen profiling (also known as 'smart controls') and how government agencies should or can work with these controls, and propose the legislative amendments needed.
15. The Government's digital strategy should be supplemented with an indicative objective with the express ambition that Sweden should become a world leader in terms of both using the opportunities offered by digitalisation and protecting privacy.

Consumers (chapter 9)

16. The Government should task the Swedish Consumer Agency with initiating and supporting the drafting of codes of conduct for industries in which personal data is processed mainly for commercial purposes.

17. The Government should task the Swedish Consumer Agency with exercising supervision of developments, products and agreements in which privacy protection and information security apply.

Insurance activities (chapter 10)

18. The Swedish Consumer Agency should monitor insurance companies' work on industry recommendations.
19. The Government should introduce a legal regulation on the duty of confidentiality in insurance activities.

Some other risk areas dealt with in the Committee's interim report (chapter 11)

20. The Government should look into how a secure system for issuing physical identification documents should be designed and what the state's responsibility for such a system should be.
21. The Government should look into a statutory right for natural persons to contact a person who is publishing a credit report publication to have data about themselves removed before it is published.
22. It is essential that the Government submits proposals for regulations that provide privacy protection when credit reports are made public, regardless of how they are made public. This can be done on the basis of proposals already submitted.
23. The Government should look into a legislative regulation of such surveillance methods used by the police that are sensitive in terms of privacy and that are currently not regulated or that are subject to weak regulation.

Information security (chapter 12)

24. The Government should investigate the proposal presented in SOU 2015:23 that the Swedish Civil Contingencies Agency should exercise supervision of government agencies' information security work in the way proposed in SOU 2015:23.

25. Regarding relevant agencies under the Government, the Government should instruct the Swedish Civil Contingencies Agency to monitor which measures government agencies are taking to comply with the Swedish Civil Contingencies Agency's regulations on government agencies' information security (MSBFS 2016:1).

26. The measures to achieve codes of conduct proposed by the Committee in other chapters of this report should include information security activities as prominent elements. If the activities are implemented, this may lead to a general improvement of the conditions for better information security in society.

27. The Government should instruct the Swedish Civil Contingencies Agency to work with other agencies to devise, administer and further develop a governance model for state information security, in line with the proposals in SOU 2015:23.

Society's protection mechanisms (chapter 13)

28. The Government should look into whether the Swedish Data Protection Authority should be given the right to bring a court action in selected compensation matters on behalf of a private individual.

29. The Government should task The Swedish Data Protection Authority with submitting annual reports to the Government on whether legal remedies are effective for protecting the rights of data subjects.

30. The Government should monitor compliance with the recommendations of the Swedish National Audit Office concerning skills and methods for investigating IT-related crime and then report the results to the Riksdag.

31. The Government should task an agency with looking into how a national education initiative should be organised and designed, and what scope and financing such an initiative should have.

Supervisory authority (chapter 14)

32. The Government should task the Swedish Agency for Public Management with conducting an agency analysis of the Swedish Data Protection Authority in line with the model it presented to the Government in December 2008 in the report entitled 'Model for agency analyses' (2008:17).

Research into privacy (chapter 15)

33. The Government should task special research appropriation to be allocated by the Swedish Research Council.
34. The Government should task Vinnova (Sweden's innovation agency) to promote projects that involve privacy enhancing technologies and working practices, to inform about the data protection regulation and to take account of the regulation when considering calls for proposals.

Evaluation of constitutional protection (chapter 16)

35. The Government should introduce a provision in the Committees Ordinance (1998:1474) stating that if the proposals in a report have a bearing on privacy in the cases referred to in Chapter 2, Article 6, second paragraph of the Instrument of Government, the consequences in this regard must be described in the report.
36. The Government should evaluate, develop and, if necessary, update the guidance document for privacy analysis issued by the Swedish Data Protection Authority.

1 Författningsförslag

Förslag till förordning om ändring i kommittéförordningen (1998:1474)

Härigenom föreskrivs i fråga om kommittéförordningen (1998:1474) att 15 § ska ha följande lydelse.

15 §

Om förslagen i ett betänkande har betydelse för den kommunala självstyrelsen, skall konsekvenserna i det avseendet anges i betänkandet. Detsamma gäller när ett förslag har betydelse för brottsligheten och det brottsförebyggande arbetet, för sysselsättning och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags, för jämställdheten mellan kvinnor och män, *eller* för möjligheterna att nå de integrationspolitiska målen.	Om förslagen i ett betänkande har betydelse för den kommunala självstyrelsen, skall konsekvenserna i det avseendet anges i betänkandet. Detsamma gäller när ett förslag har betydelse för brottsligheten och det brottsförebyggande arbetet, för sysselsättning och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags, för jämställdheten mellan kvinnor och män, för möjligheterna att nå de integrationspolitiska målen *eller för den personliga integriteten i de fall som avses i 2 kap. 6 § andra stycket regeringsformen*.

Denna förordning träder i kraft den 1 juli 2018.

DEL II

Integritetskommitténs uppdrag och arbete m.m.

2 Integritetskommitténs utgångspunkter, uppdrag och arbete

2.1 Kommitténs uppdrag

Kommitténs tre primära uppdrag har varit att

- utifrån ett individperspektiv, kartlägga och analysera faktiska och potentiella risker för intrång i den personliga integriteten i samband med användning av informationsteknik,
- bedöma behovet av att inrätta ett s.k. integritetsskyddsråd, vars syfte skulle vara att höja kvaliteten i lagstiftningsprocessen, när det gäller lagförslag som påverkar den personliga integriteten, och
- följa upp effekterna i lagstiftningsarbetet av den förstärkning av grundlagsskyddet, som genomfördes 2011.

De två förstnämnda uppdragen har presenterats i delbetänkandet,[1] medan analysen av grundlagsförstärkningen behandlas i detta slutbetänkande. Här fullföljer kommittén även sin analys av faktiska och potentiella risker genom att med utgångspunkt från den genomförda kartläggningen framföra förslag till åtgärder, redovisa konsekvenserna av dessa samt ange förslag till finansiering.

[1] *Hur står det till med den personliga integriteten?* (SOU 2016:41).

2.2 Kommitténs sammantagna bedömning

Integritetskommittén redovisade i delbetänkandet[2] sin bedömning av den samlade effekten av den kartläggning och övervakning som en enskild person blir föremål för i dagens digitaliserade samhälle.

Kommitténs generella slutsats är att den enskilde på ett flertal områden drabbas av stegvisa försämringar av den personliga integriteten. Den enskildes kunskaper om hur dennes personuppgifter hanteras och enskildas möjligheter att påverka hur och vem som använder dem, försämras kontinuerligt. Det beror bland annat på att tillämpningen av de grundläggande skyddsbestämmelserna om information, samtycke, angivande av ändamål och gallring försvagats i takt med den digitala expansionen.

Det centrala problemet här är således inte avsaknaden av ett regelverk, utan snarare bristen på efterlevnad. Den här bristen har vi kunnat konstatera inom samtliga samhällsområden, såväl inom myndigheter, kommuner och landsting som hos kommersiella aktörer. Ett regelverk med normer som inte följs eller är svåra att följa skadar respekten för regelverket; både hos dem som ska tillämpa reglerna och de som ska skyddas av dem. Vissa personuppgiftsansvariga kanske inte ens ser det som meningsfullt att följa reglerna, eftersom allmänheten, eller åtminstone en tillräckligt stor andel, inte tydligt ställer det kravet. Till detta ska läggas att den som begår överträdelser löper en förhållandevis liten risk för att upptäckas och drabbas av sanktioner.

2.3 Målet med kommitténs arbete

2.3.1 Den enskildes ställning behöver stärkas

Kommittén har formulerat följande övergripande mål för sitt arbete:

> Skyddet av den personliga integriteten ska stärkas så att denna grundläggande rättighet är i balans med andra grundläggande rättigheter och legitima samhällsintressen.

[2] SOU 2016:41, s. 49 ff.

Vi tror att ett stärkande av den enskildes ställning gentemot den personuppgiftsansvarige är av grundläggande betydelse för att vända utvecklingen. Den enskildes möjlighet till kunskap om att dennes personuppgifter används och förståelse för hur de används behöver därför förbättras. Först då kan en enskild användare ta reell ställning till de erbjudanden som ges och få ett rimligt inflytande över behandlingen av personuppgifter. Med ökad kunskap följer också en ökad förmåga att ställa krav på dem som tillhandahåller digitala tjänster, vilket i sin tur bör leda till att dessa aktörer drivs att erbjuda ett fullgott integritetsskydd av kommersiella skäl. Integritetsskydd och tillit till den erbjudna produkten blir då ett konkurrensmedel. Kommittén anser därför att särskilda insatser för att höja den allmänna kunskapsnivån bör genomföras.

2.3.2 Behov av kraftsamling

För att nå upp till kommitténs ambitiösa mål att bryta den i delbetänkandet beskrivna utvecklingen behövs en kraftsamling inom en rad områden. Med tanke på att dataskyddsförordningen ska börja tillämpas i maj 2018, är tidpunkten för en sådan kraftsamling just nu mycket lämplig. Ett förverkligande av intentionerna bakom den nya förordningen förutsätter betydande insatser inom samtliga samhällsområden.

De förslag som kommittén i det följande lägger fram utgår från den riskbedömning som gjordes i delbetänkandet med ett särskilt fokus på de områden och företeelser, där vi funnit allvarliga eller påtagliga risker för den personliga integriteten. Vi har också prioriterat grupper som är särskilt utsatta eller skyddsvärda.

Kommitténs uppdrag täcker ett mycket vidsträckt område. Det har därför inte varit möjligt att med den tid, som avsatts för det här uppdraget, utarbeta fullständiga förslag till åtgärder. I flera fall förutsätter därför våra förslag ytterligare utredning innan de kan realiseras.

Det pågår för närvarande ett stort antal utredningar, som har beröringspunkter med den här utredningen. Vi avstår självfallet från att lägga förslag, som skulle kunna kollidera med dessa utredningars

direktiv. Ett exempel på detta är den pågående Forskningsdatautredningen.[3]

I den tidigare kartläggningen konstaterade kommittén att många av de påtalade problemen är av det slaget att de inte kan lösas av en enskild stat. Samverkan på internationell nivå och utarbetande av gemensamma normer och synsätt är därför mycket viktigt. Förslagen i det här betänkandet tar dock främst sikte på åtgärder, som kan vidtas inom landet.

Som redan nämnts är regelefterlevnad ett återkommande problem. Det handlar inte bara om okunskap och en ovilja att följa regelverket utan också om att bestämmelserna i många avseenden är medvetet oprecisa och allmänt formulerade och därmed svåra att tillämpa. Här anger dataskyddsförordningen nya arbetssätt såsom upprättande av uppförandekoder, vilket är ett slag av branschvis självreglering i syfte att konkretisera regelverket. Vi tror att uppförandekoder kan bli ett effektivt hjälpmedel för att höja skyddet av den personliga integriteten inom flera områden.

2.4 Verksamheter som vi anser är särskilt viktiga att åtgärda

2.4.1 E-förvaltning

Inom stat och kommun hanteras stora mängder personuppgifter, ofta av känslig natur. Den enskilde har i allmänhet inget inflytande över myndigheternas hantering. Det vilar därför ett särskilt ansvar på myndigheterna att se till att uppgifter bara hanteras när det är nödvändigt och att se till att hanteringen är så säker som möjligt. Regeringen har uttalat mycket höga ambitioner när det gäller utvecklingen och digitaliseringen av den offentliga sektorn. Kommittén ser ett starkt behov av att regeringen uttalar lika höga ambitioner när det gäller den tekniska säkerheten och skyddet av personuppgifter inom det här området samt att tillräckliga resurser avsätts för att möjliggöra detta.

[3] U 2016:04, dir. 2016:65. Utredaren ska bl.a. lämna förslag på sådana lämpliga skyddsåtgärder för den registrerades fri- och rättigheter som behandling av personuppgifter för forskningsändamål ska omfattas av.

2.4.2 Konsumentområdet

Kommittén har konstaterat att den enskilde utsätts för allvarliga risker för den personliga integriteten i sin egenskap av konsument och användare av sociala medier. I allt väsentligt är det personuppgiftslagen och från maj 2018 dataskyddsförordningen som reglerar personuppgiftsbehandlingen inom det här området. Även om förordningen ställer en del specifika krav på de ansvariga, är många bestämmelser allmänt hållna. Vi tror därför att proaktiva insatser för att få till stånd uppförandekoder inom det här området är särskilt angeläget.

2.4.3 Informationssäkerhet

Kommittén har konstaterat att det finns starka indikationer på väsentliga brister i informationssäkerheten över hela den offentliga sektorn. Förhållandena på den privata sektorn är svårare att uttala sig om på ett generellt plan, bl.a. beroende på bristen på granskningar inom det området.

Det pågår för närvarande en hel del utredningar och andra aktiviteter inom det här området för att förbättra situationen. Kommittén bedömer att en god informationssäkerhet är av avgörande betydelse för att skyddet för den personliga integriteten ska kunna stärkas.

2.4.4 Tillsynsmyndigheten

Den kommande dataskyddsförordningen kan bli ett effektivt medel för att stärka skyddet av den personliga integriteten, men det ligger förvisso ingen automatik i detta. För att höja efterlevnaden och medvetenheten i hela samhället av de sedan länge gällande principerna om information, samtycke, berättigat ändamål och gallring krävs bland annat en aktiv tillsyn. När man dessutom ska etablera de delvis nya reglerna om ansvarighet, konsekvensbedömningar, förhandssamråd, rapportering av personuppgiftsincidenter, inbyggd integritet, uppförandekoder m.m. krävs en aktiv och närvarande tillsynsmyndighet med betydligt större resurser än den har i dag.

2.4.5 Forskning om digitalisering och integritet

Kommittén konstaterade i delbetänkandet att det är förhållandevis lite forskning som har bedrivits om vilken inverkan den digitala utvecklingen har på människan och hennes uppfattning om världen och om sig själv. Kommittén noterade också att forskningen är tämligen strikt uppdelad, för att inte säga separerad i tre vetenskapliga fält, nämligen teknik, juridik och samhällsvetenskap. Forskning om digitalisering och personlig integritet är ett område som förtjänar större uppmärksamhet; både för att höja kunskapsnivån men också för att bidra till att finna lösningar av tekniska och legala utmaningar.

2.5 Det fortsatta arbetet

Sammanfattningsvis innehåller kommitténs kraftsamling för stärkande av den personliga integriteten ett 30-tal olika förslag inom flera departementsområden. Ett begränsat antal av förslagen avser ny eller ändrad lagstiftning. Flertalet faller inom ramen för regeringens myndighetsstyrning. För att den här breda ansatsen ska bli praktiskt möjlig att genomföra, bedömer kommittén att man inom Regeringskansliet bör inrätta en tillfällig projektgrupp med företrädare för berörda departement, som ges i uppdrag att vidareutveckla, samordna, genomföra och följa upp de aktiviteter, som regeringen väljer att gå vidare med.

Kommittén är medveten om att huvuddelen av de förslag, som läggs, naturligen bereds först i samband med budgetprocessen för år 2019. Kommittén vill dock starkt plädera för att två frågor bereds omgående, nämligen avsättningen av medel för att uppmuntra framtagandet av uppförandekoder samt uppdraget till Statskontoret att genomföra en myndighetsanalys av Datainspektionen. Frågan om uppförandekoderna bör kunna beredas redan i vårpropositionen 2018 och uppdraget till Statskontoret skulle kunna inledas t.o.m. före dess. Båda dessa förslag hänger intimt samman med att dataskyddsförordningen ska börja tillämpas redan i maj 2018. Det vore därför olyckligt att skjuta upp dessa delar till 2019.

Som framgår nedan lägger kommittén inte förslag inom samtliga områden, som har granskats. Det är kommitténs starka förhoppning att den genomförda kartläggningen ändå ska vara till nytta och kunna ligga till grund för insatser och förbättringar inom respektive om-

råde. I den mån det finns en utpekad ansvarig myndighet kan kartläggningen användas för att rikta särskilda regeringsuppdrag. Den skulle också kunna användas av tillsynsmyndigheten vid urvalet av kommande tillsynsinsatser.

När det gäller till exempel personuppgiftsbehandlingen inom polisen anser kommittén att det finns anledning för regeringen att följa polisens förbättringsarbete vad gäller följsamheten till integritetsskyddslagstiftningen.

2.6 Integritetskommitténs arbete med betänkandet

Integritetskommitténs uppdrag har omfattat personuppgiftsbehandling inom i princip alla samhällsområden. Kommittén har avstått från att fördjupa sig i områden, som andra utredningar ägnar sig åt men däremot fortlöpande följt dessas arbete.

Det som redovisas här, är endast de möten och kontakter som kommittén eller sekretariatet haft i samband med arbetet med slutbetänkandet. Kommitténs tidigare möten och kontakter redovisades i delbetänkandet.

Integritetskommittén har träffats vid sju tillfällen och sekretariatet har träffat expertgruppen vid fyra tillfällen.

Därutöver har sekretariatet haft kontakter med, bland andra, följande utredningar: *Dataskyddsutredningen*[4], *Utredningen om genomförande av NIS-direktivet*[5], *Forskningsdatautredningen*[6], *Socialdataskyddsutredningen*[7], *Utbildningsdatautredningen*[8] och *Utredningen om effektiv styrning av nationella digitala tjänster*[9].

Det i direktivet föreskrivna samrådet med Datainspektionen och Post- och Telestyrelsen har fullgjorts genom att dessa två myndigheter varit representerade i utredningens expertgrupp.

Dessutom har sekretariatet haft kontakt med bland andra Skolverket, Konsumentverket, E-hälsomyndigheten, Arbetsmiljöverket, Statens servicecenter, Sveriges kommuner och landsting (SKL), olika

[4] Ju 2016:04.
[5] Ju 2016:11.
[6] U 2016:04.
[7] S 2016:05.
[8] U 2016:03.
[9] N 2016:01.

tjänstleverantörer och branschorganisationer samt vissa arbetsgivarorganisationer och fackliga organisationer.

Kommitténs ordförande och sekretariatet har deltagit i olika konferenser och seminarier med anknytning till utredningsuppdraget.

2.7 Betänkandets disposition

I delbetänkandet beskrev vi riskerna för den enskilde individens integritet i olika samhällssektorer och även i samband med olika företeelser som är särskilt intressanta ur integritetssynpunkt. De förslag som kommittén nu presenterar utgår från den riskbedömning som gjordes i delbetänkandet med ett särskilt fokus på de områden och företeelser, där vi funnit allvarliga eller påtagliga risker för den personliga integriteten. Förslagen är indelade i samma verksamhetsområden som i delbetänkandet.

Betänkandet är uppdelat i fyra delar.

Del I *Inledning* omfattar Sammanfattning, en engelsk översättning av denna och Författningsförslag (kapitel 1)

Del II *Integritetskommitténs uppdrag och arbete m.m.* omfattar kapitel 2–4. Denna del inleds med detta kapitel (kapitel 2). Därefter följer kapitlet Något om de nya kraven i dataskyddsförordningen (kapitel 3) där kommittén beskriver på vilket sätt förordningen kan vara ett stöd i arbetet med att stärka den enskildes integritet. Därefter kommer kapitel 4 Uppförandekoder i dataskyddsförordningens mening.

Del III *Kommitténs förslag* omfattar kapitel 5–17. I kapitel 5–11 redogör kommittén för sina förslag till åtgärder för att stärka den enskildes integritet inom olika sektorer av samhället.

Kapitel 12 handlar om informationssäkerhet och vilka åtgärder som behövs för att stärka detta arbete. Kapitel 13 handlar om samhällets skyddsmekanismer. Därefter kommer kapitel 14 om tillsynsmyndigheten och kapitel 15 handlar om forskning om personlig integritet. I kapitel 16 redogör vi för vår utvärdering av grundlagsskyddet. Det sista kapitlet (17) utgör en konsekvensbeskrivning av våra förslag.

Bilagorna till betänkandet presenteras i del IV.

3 Något om de nya kraven i dataskyddsförordningen

3.1 Ny lagstiftning – nya möjligheter

Dataskyddsförordningen ska börja tillämpas den 25 maj 2018. Personuppgiftslagen kommer då att upphöra att gälla och en mängd lagar och andra regler kommer att ha anpassats till att vi har direktverkande EU-regler i stället.

Arbetet med att anpassa regelverk och verksamhetsrutiner till dataskyddsförordningen pågår nu för fullt, både hos lagstiftaren genom ett flertal olika statliga utredningar och hos myndigheter och privata verksamheter.

Integritetskommittén anser att regeringen, myndigheterna och företagen bör ta detta tillfälle i akt och använda arbetet med införandet av förordningen som en möjlighet att ta ett nytt och starkt grepp om dataskyddet. Det är ett utmärkt tillfälle att lyfta de personuppgiftsansvarigas arbete med en säker och ändamålsenlig informationshantering till en högre nivå.

Innebörden av dataskyddsförordningens bestämmelser måste därför göras lätt tillgängliga för de personuppgiftsansvariga och för allmänheten. Kraven och de möjligheter till bättre dataskydd som dessa innebär måste göras allmänt kända. Detta är en naturlig arbetsuppgift för Datainspektionen.

Den s.k. Artikel 29-gruppen[1] har givit ut flera vägledningar för hur vissa bestämmelser i förordningen ska tillämpas. Under det närmaste

[1] Artikel 29-gruppen är en rådgivande och oberoende arbetsgrupp som bland annat har till uppgift att utreda frågor som rör tillämpningen av EU:s dataskyddsdirektiv 95/46 samt att ge råd om andra föreslagna åtgärder inom EU med avseende på behandling av personuppgifter. Gruppen består av representanter för samtliga dataskyddsmyndigheter i EU:s medlemsstater samt representanter för den Europeisk datatillsynsmannen (EDPS) och EU-kommissionen.

året planerar gruppen att ge ut vägledningar om fler frågor om förordningens tillämpning.

I detta kapitel uppmärksammar vi några viktiga nyheter i dataskyddsförordningen, jämfört med dagens regelverk (dataskyddsdirektivet och personuppgiftslagen). Flera av de nya bestämmelserna har betydelse för våra förslag och bedömningar i detta slutbetänkande.

3.2 Ansvarsskyldighet

En ny princip

Ett nytt krav i dataskyddsförordningen, är att den personuppgiftsansvarige ska *ansvara för* och *kunna visa* att den följer förordningens principer för behandling av personuppgifter. Det nya kravet omtalas i bland i termer av en ny princip, vilken då kallas för principen om *ansvarsskyldighet*.

Det verkligt nya består här i skyldigheten att kunna visa att regelverket följs. Andra bestämmelser i förordningen pekar på hur detta kan gå till. Exempelvis är ett sätt för den personuppgiftsansvarige att visa detta, att ansluta sig till en godkänd uppförandekod eller en godkänd certifieringsmekanism (art 24.3 och art 32.3).

Även för ett personuppgiftsbiträde kan anslutningen till en godkänd uppförandekod eller en godkänd certifieringsmekanism vara ett sätt att visa att biträdet tillhandahåller tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i förordningen och säkerställer att den registrerades rättigheter skyddas (art 28.5).

Systematiskt arbete med dataskydd och informationssäkerhet

Dataskyddsförordningens krav att den personuppgiftsansvarige ska ansvara för och kunna visa att den följer förordningen, kan jämföras med krav som redan i dag gäller inom några närliggande områden, där ledningssystem ska användas för att tydliggöra myndighetens ansvar.

Myndighetens för samhällsskydd och beredskap (MSB) definierar ett ledningssystem för informationssäkerhet som ett sätt för organisationens ledning att på ett systematiskt sätt styra arbetet

med informationssäkerhet i syfte att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamhetens informationshantering.

För statliga myndigheter finns det exempelvis krav i MSB:s föreskrifter (MSBFS 2016:1) om statliga myndigheters informationssäkerhet. Enligt dessa ska statliga myndigheter bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet. I detta arbete ska standarderna ISO/IEC 27001:2014 och ISO/IEC 27002:2014 beaktas. Genom ledningssystemet ska myndigheten bland annat tydliggöra myndighetsledningens och den övriga organisationens ansvar för myndighetens informationssäkerhetsarbete. Vidare ska enligt föreskrifterna tillräckliga resurser tilldelas för informationssäkerhetsarbetet. Dessutom ska löpande och regelbunden information lämnas till myndighetsledningen om detta arbete.

Krav på ledningssystemet finns även i Socialstyrelsens föreskrifter och allmänna råd (SOSFS 2011:9) om ledningssystem för systematiskt kvalitetsarbete. Enligt Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården, ska en vårdgivare genom sitt ledningssystem säkerställa informationssäkerheten vid behandling av personuppgifter. Vårdgivaren bör enligt det allmänna rådet till bestämmelsen använda svenska standarder för informationssäkerhet då ledningssystemet byggs upp. Sådana standarder kan vara standarder i ISO/IEC 27000-serien.

Innebörden av ett systematiskt arbete

För ledningen av en verksamhet är alltså kraven på ett systematiskt arbetssätt för att styra och leda inom ett visst område ofta inte något främmande. Genom att använda sig av ett systematiskt kvalitetsarbete även när det gäller dataskydd och informationssäkerhet, har ledningen för en verksamhet goda förutsättningar för att kunna visa att den följer dataskyddsförordningens bestämmelser.

Det bör dock betonas att ett systematiskt arbete med dataskydd och informationssäkerhet inte per automatik innebär att dataskyddsförordningens krav är uppfyllda – verksamheten måste också i den

konkreta tillämpningen behandla uppgifterna i enlighet med dataskyddsförordningens materiella bestämmelser.

3.3 Information till de registrerade

Den personuppgiftsansvarige ska enligt dataskyddsförordningens artikel 12 (skäl 58–59) vidta lämpliga åtgärder så att den registrerade får all information och kommunikation om behandlingen, som han eller hon har rätt till. Den ska ges i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av ett klart och tydligt språk.

Detta gäller i synnerhet för information som är särskilt riktad till barn. Informationen ska ges skriftligt, eller i någon annan form. När det är lämpligt ska den ges elektroniskt. Om den registrerade begär det, får informationen ges muntligt, förutsatt att den registrerades identitet bevisats.

3.4 Samtycke

I dataskyddsförordningen anges på ett tydligare sätt än i dataskyddsdirektivet vad som kan utgöra ett giltigt samtycke.

I artikel 7.1 anges att om den registrerades samtycke lämnas i en skriftlig förklaring som också rör andra frågor, ska begäran om samtycke läggas fram på ett sätt som klart och tydligt kan särskiljas från de andra frågorna i en begriplig och lätt tillgänglig form, med användning av ett klart och tydligt språk.

Vidare ska enligt artikel 7.4 vid bedömning av om samtycke är frivilligt, största hänsyn bland annat tas till om genomförandet av ett avtal, inbegripet tillhandahållandet av en tjänst, har gjorts beroende av samtycke till sådan behandling av personuppgifter som inte är nödvändig för genomförandet av det avtalet.

I skälen till förordningen anges även att tystnad, på förhand ikryssade rutor eller inaktivitet inte bör utgöra samtycke.[2] Vidare anges i skälen att samtycke inte antas vara frivilligt om det inte medger att separata samtycken lämnas för olika behandlingar av person-

[2] Skäl 32.

uppgifter, trots att detta är lämpligt i det enskilda fallet. Inte heller anses samtycket vara frivilligt om genomförandet av ett avtal – inbegripet tillhandahållandet av en tjänst – är avhängigt av samtycket, trots att samtycket inte är nödvändigt för ett sådant genomförande.[3]

Dataskyddsförordningen innehåller också bestämmelser om villkor för barns samtycke avseende informationssamhällets tjänster (exempelvis olika sociala medier).[4]

3.5 Konsekvensbedömningar

Dataskyddsförordningen innehåller ett krav på den personuppgiftsansvarige att göra en konsekvensbedömning avseende dataskydd i vissa situationer (artikel 35). Ett sådant, uttryckligt krav finns inte i dataskyddsdirektivet, även om konsekvensbedömningar av detta slag inte är ovanliga redan i dag.

Den vanligaste, engelska benämningen på företeelsen är *privacy impact assessment.* I dataskyddsförordningens engelska språkversion används uttrycket *data protection impact assessment.*

Bestämmelsen innebär att, om en personuppgiftsansvarig planerar en typ av behandling som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter, ska denne före behandlingen göra en bedömning av behandlingens konsekvenser för skyddet av personuppgifterna. Detta är särskilt viktigt i samband med användning av ny teknik. Vilken typ av behandling det handlar om, vilken omfattning den har och i vilket sammanhang och för vilket ändamål, kan också vara omständigheter som bör leda till att en konsekvensbedömning avseende dataskydd ska göras. Den personuppgiftsansvarige ska rådfråga dataskyddsombudet vid genomförandet av konsekvensbedömningen.

Artikel 29-gruppen har gett ut en vägledning för konsekvensbedömningar enligt dataskyddsförordningen[5] samt en vägledning om dataskyddsombud.[6]

[3] Skäl 43.
[4] Artikel 8.
[5] WP 248, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, April 2017.
[6] WP 243 rev.01, *Guidelines on Data Protection Officers ('DPOs')*, April 2017.

Konsekvensbedömningar enligt andra regelverk

För många verksamheter är det inget nytt eller främmande krav att göra en konsekvensbedömning i form av en riskanalys inför exempelvis förändringar i verksamheten eller inför införande av nya metoder och liknande.

Riskanalyser ingår dessutom i ett systematiskt informationssäkerhetsarbete. För statliga myndigheter finns det exempelvis krav i MSB:s ovan nämnda föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1). Enligt dessa ska statliga myndigheter bedriva ett systematiskt och *riskbaserat* informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet. Enligt föreskriften ska myndigheterna i syfte att hantera hot och risker som rör informationssäkerheten i verksamheten bland annat klassa information med utgångspunkt i konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser som kan uppstå av ett bristande skydd, samt identifiera, analysera och bedöma hot och risker för verksamhetens information, system och tjänster.

Ett annat exempel är att vårdgivare eller de som bedriver socialtjänst enligt 5 kap. 1 § Socialstyrelsens föreskrifter och allmänna råd (SOSFS 2011:9) om ledningssystem för systematiskt kvalitetsarbete, fortlöpande ska bedöma om det finns risk för att händelser skulle kunna inträffa som kan medföra brister i verksamhetens kvalitet.

Tillsynsmyndigheten (som i Sverige föreslås bli Datainspektionen[7]) ska enligt artikel 35.4 upprätta och offentliggöra en förteckning över det slags behandlingsverksamheter som omfattas av kravet på en konsekvensbedömning avseende dataskydd. Myndigheten får också föra en förteckning över sådana behandlingar som *inte* kräver någon konsekvensbedömning (artikel 35.5).

[7] Utredningens om tillsynen över den personliga integriteten betänkande, *Ett samlat ansvar för tillsyn över den personliga integriteten* (SOU 2016:65) och Dataskyddsutredningens betänkande, *Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning* (SOU 2017:39). När tillsynsmyndigheten enligt dataskyddsförordningen berörs i det som följer, omnämner vi den ibland som Datainspektionen.

3.6 Förhandssamråd

Förhandssamråd regleras i artikel 36 i dataskyddsförordningen, och kommenteras i skäl 94. Av artikeln framgår att den personuppgiftsansvarige ska samråda med tillsynsmyndigheten före en behandling av personuppgifter om en konsekvensbedömning visar att behandlingen skulle leda till en hög risk, om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken.

Om tillsynsmyndigheten anser att den planerade behandlingen skulle strida mot förordningen, ska myndigheten ge den personuppgiftsansvarige och personuppgiftsbiträdet skriftliga råd och utnyttja alla sina befogenheter enligt artikel 58 (exempelvis att begära mer information, att förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att se till att behandlingen görs i enlighet med förordningen, eller att införa en begränsning av behandlingen).

3.7 Personuppgiftsincidenter

Genom dataskyddsförordningen införs en skyldighet för den personuppgiftsansvarige att anmäla till tillsynsmyndigheten om det inträffar en så kallad personuppgiftsincident. Detta är i dataskyddsförordningen en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som behandlats. Även den registrerade ska informeras om incidenten om den sannolikt leder till en hög risk för enskildas rättigheter och friheter. Detta regleras i artikel 33 och 34 (skäl 85–88).

Avvikelserapportering i andra sammanhang

Med avvikelse avses i flera sammanhang att verksamheten inte når upp till krav och mål enligt lagar och andra föreskrifter och beslut som har meddelats med stöd av sådana föreskrifter.

Krav på incidentrapportering finns i MSB:s föreskrifter (MSBFS 2016:2) om statliga myndigheters rapportering av it-incidenter. Här ges föreskrifter om hur statliga myndigheter till MSB ska rapportera it-incidenter som allvarligt kan påverka säkerheten i den infor-

mationshantering som myndigheten ansvarar för, eller i tjänster som myndigheten levererar till en annan organisation.

Krav på intern incidenthantering finns i MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1). En myndighet ska enligt dessa ha rutiner för att identifiera, rapportera, bedöma, hantera och dokumentera incidenter som kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation. Myndigheten ska ha rutiner för att lära av sådana inträffade incidenter och utförda åtgärder.

I hälso- och sjukvårdslagstiftningen finns exempelvis bestämmelser som reglerar skyldigheter att rapportera vårdskador och risker för vårdskador. Vårdgivaren har som ansvarig för verksamheten en skyldighet att utreda rapporter om händelser som medfört eller hade kunnat medföra en vårdskada.

Framkomna avvikelser ska även medföra att den som bedriver verksamhet ser över sina processer och rutiner. Visar avvikelserna att processer och rutiner inte är ändamålsenliga för att säkra verksamhetens kvalitet så ska dessa förbättras. Detta innebär att verksamheten blir en lärande organisation. Utifrån framkomna avvikelser förbättras fortlöpande verksamhetens styrning så att liknande avvikelser inte återupprepas. Därmed utvecklas och säkras verksamhetens kvalitet.

Att en avvikelse inträffar i en verksamhet är något negativt. Men som en del av ett systematiskt förbättringsarbete är det viktigt att betona att varje upptäckt av en sådan avvikelse är något positivt. Genom upptäckten av en avvikelse säkerställs dels att den kan åtgärdas, dels att verksamheten får en möjlighet att se över sin styrning och därigenom kan förhindra att liknande avvikelser återupprepas.

3.8 Inbyggt dataskydd och dataskydd som standard

Dataskyddsförordningen innehåller till skillnad från dataskyddsdirektivet uttryckliga krav på s.k. inbyggt dataskydd (på engelska *privacy by design*) och dataskydd som standard (på engelska *privacy by default*).

Enligt artikel 25 ska den personuppgiftsansvarige bland annat, med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt ris-

kerna för fysiska personers rättigheter och friheter, genomföra lämpliga tekniska och organisatoriska åtgärder – såsom pseudonymisering – vilka är utformade för ett effektivt genomförande av dataskyddsprinciper – såsom uppgiftsminimering – och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, så att kraven i dataskyddsförordningen uppfylls och den registrerades rättigheter skyddas. Detta kan också uttryckas som att den personuppgiftsansvarige ska låta integritetsfrågor påverka ett it-systems hela livscykel – från förstudie och kravställning via design och utveckling till användning och avveckling.[8]

Den personuppgiftsansvarige ska enligt artikel 25 också genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Framför allt ska säkerställas att personuppgifter (i standardfallet) inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.

3.9 Uppförandekoder och certifieringar

I syfte att specificera hur dataskyddsförordningen ska tillämpas inom en viss bransch eller sektor, får sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden, utarbeta uppförandekoder (artikel 40). Uppförandekoder behandlas mer ingående i kapitel 4.

Dataskyddsförordningen innehåller också bestämmelser om certifieringar (artikel 41). Dessa är certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd som syftar till att visa att personuppgiftsansvarigas eller personuppgiftsbiträdens behandling är förenlig med dataskyddsförordningen. Medlemsstaterna, tillsynsmyndigheterna, dataskyddsstyrelsen och kommissionen ska uppmuntra, särskilt på unionsnivå, införandet av certifieringsmekanismer. Förordningen innehåller också bestämmelser om hur och av vem certifiering kan utfärdas.

[8] Se Datainspektionens informationsbroschyr *Inbyggd integritet* (januari 2012).

3.10 Sanktionsavgifter

Genom dataskyddsförordningen införs en skyldighet för tillsynsmyndigheten att i vissa situationer besluta om administrativa sanktionsavgifter på upp till 20 miljoner euro eller 4 procent av organisationens omsättning när en organisation missköter sin behandling av personuppgifter. Det saknas någon motsvarande bestämmelse i dataskyddsdirektivet.

I förordningens artikel 83 föreskrivs att varje tillsynsmyndighet ska säkerställa att påförande av administrativa sanktionsavgifter i varje enskilt fall är effektivt, proportionellt och avskräckande.

3.11 Dataportabilitet

Dataskyddsförordningen innehåller en förstärkning av rätten att få åtkomst till sina personuppgifter när syftet är att föra över dem till en annan leverantör av elektroniska tjänster, så kallad dataportabilitet (artikel 20).

Rättigheten innebär att den registrerade som huvudregel ska ha rätt att få ut de personuppgifter som rör honom eller henne och som han eller hon har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format. Den registrerade har rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan att den personuppgiftsansvarige som tillhandahållits personuppgifterna hindrar detta. Allmänna förutsättningar för rätten till dataportabilitet, är att behandlingen grundar sig på samtycke enligt artikel 6.1 a eller artikel 9.2 a eller på ett avtal enligt artikel 6.1 b, och att behandlingen görs automatiserat.[9]

Artikel 29-gruppen har gett ut en vägledning för tillämpningen av bestämmelserna om dataportabilitet.[10]

[9] Artikel 20.
[10] WP 242 rev.01, *Guidelines on the right to data portability*, April 2017.

4 Allmänt om uppförandekoder

4.1 Uppförandekoder i dataskyddsförordningen och dataskyddsdirektivet

I dataskyddsförordningens artikel 40 sägs att medlemsstaterna, tillsynsmyndigheterna, styrelsen och kommissionen ska uppmuntra utarbetandet av uppförandekoder avsedda att bidra till att förordningen genomförs korrekt, med hänsyn till särdragen hos de olika sektorer där behandling sker, och de särskilda behoven hos mikroföretag samt små och medelstora företag. Vidare sägs att sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden får utarbeta uppförandekoder, eller ändra eller utöka sådana koder, i syfte att specificera tillämpningen av förordningen.

En uppförandekod är således enligt dataskyddsförordningen en möjlighet för sammanslutningar som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden inom en viss bransch eller sektor, att specificera hur man i praktiken ska tillämpa dataskyddsförordningens bestämmelser, som i många avseenden är allmänt hållna. Uppförandekoder är möjliga även om det finns nationella bestämmelser som, med stöd i dataskyddsförordningen, närmare reglerar hur uppgifter får behandlas inom en sektor.

Uppförandekoder kan även omfatta verksamhet som bedrivs av myndigheter.

I det regelverk som tillämpas i dag, motsvaras dataskyddsförordningens uppförandekoder närmast av de ”branschöverenskommelser” som nämns i den svenska personuppgiftsförordningen (1998:1191) som gäller i dag och fram till den 25 maj 2018, då dataskyddsförordningen ska börja tillämpas. Enligt 15 § personuppgiftsförordningen ska Datainspektionen på begäran av en organisation som företräder en väsentlig del av de personuppgiftsansvariga inom en viss

bransch eller inom ett visst område avge yttrande över förslag till överenskommelser vad avser behandling av personuppgifter inom branschen eller området (branschöverenskommelse).

Beteckningen ”branschöverenskommelse” motsvaras i dataskyddsdirektivet från 1995 av begreppet ”uppförandekodex” som i allt väsentligt får anses som liktydigt med ”uppförandekod” i dataskyddsförordningen.

Det kan vara värt att notera att direktivets uppförandekodex i det svenska genomförandet fått karaktär av överenskommelse. Såväl dataskyddsdirektivet som dataskyddsförordningen saknar emellertid skrivningar om att det måste vara fråga om en överenskommelse eller ett avtal. En annan sak är att det i praktiken kan vara en stor fördel att inblandade parter är överens om innehållet i en uppförandekod. Med inblandade parter menas här branschens organisationer för personuppgiftsansvariga eller personuppgiftsbiträden, organisationer som representerar registrerade inom branschen och tillsynsmyndigheten.

Det är också värt att notera att dataskyddsförordningen föreskriver att uppförandekoderna ska ta hänsyn till de särskilda behoven hos mikroföretag samt små och medelstora företag. En uppförandekod får således inte förstärka större företags försprång när det gäller möjligheterna att påverka branschpraxis och på så sätt hindra konkurrensen. Hänsyn till mikroföretag samt små och medelstora företag innebär också att tillämpningen ska underlättas för dem som har mindre resurser att tillgå för exempelvis juridisk hjälp med att tolka och tillämpa dataskyddsförordningen.

Uppförandekoder kan på flera sätt spela en viktig roll i tillämpningen av förordningen; bland annat genom att tydliggöra hur förordningen ska tillämpas, genom att underlätta för den ansvarige att visa att och hur den följer förordningen, vid anlitandet av personuppgiftsbiträden och vid de tillfällen när det kan bli aktuellt att påföra sanktionsavgifter.

4.1.1 Initiativ till uppförandekod

Av dataskyddsförordningen framgår att de som får utarbeta uppförandekoder är sammanslutningar och andra organ, som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden.

Det är med andra ord företrädare för personuppgiftsansvariga eller personuppgiftsbiträden som står bakom en kod, och som står som författare till koden.

Många gånger är det sannolikt nödvändigt att i en uppförandekod, som ska rikta sig till de personuppgiftsansvariga, involvera även företrädare för personuppgiftsbiträden. Det är fallet inom sektorer där beroendet av externa it-leverantörer är stort, som exempelvis inom stora delar av e-förvaltningen. Det kan också vara en fördel i andra branscher där leverantörerna i praktiken har bättre kunskap än beställarna om både problem och lämpliga lösningar.

Förordningen innehåller vidare ett aktivitetskrav på både nationella myndigheter och EU-gemensamma organ när det gäller utarbetandet av uppförandekoder. I förordningens artikel 40 sägs att medlemsstaterna, tillsynsmyndigheterna, styrelsen och kommissionen ska uppmuntra utarbetandet av uppförandekoder. Att ”uppmuntra” bör enligt Integritetskommittén förstås som att de nämnda organen ska initiera och stödja företrädare för personuppgiftsansvariga eller personuppgiftsbiträden i arbetet med att ta fram uppförandekoder.

4.1.2 Uppförandekodernas innehåll

I förordningen anges ett antal exempel på frågor som kan omfattas av en uppförandekod, bland annat dessa:

- rättvis och öppen behandling av personuppgifter,
- personuppgiftsansvarigas berättigade intressen i särskilda sammanhang,
- insamling av personuppgifter,
- pseudonymisering av personuppgifter,
- information till allmänheten och de registrerade,
- utövande av registrerades rättigheter,
- information till och skydd av barn,
- metoder för att erhålla samtycke från de personer som har föräldraansvar för barn,

- åtgärder och förfaranden som avses i artiklarna 24 och 25 om de personuppgiftsansvarigas ansvar och om inbyggt dataskydd och dataskydd som standard, samt
- åtgärder för att säkerställa säkerhet vid behandling i enlighet med artikel 32.

4.1.3 Samråd med de registrerade

Vid utformningen av en uppförandekod eller vid ändring eller utvidgning av en befintlig sådan kod, bör sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden samråda med berörda intressenter. Samrådet ska i möjligaste mån inbegripa registrerade. I arbetet ska man beakta de inlagor som mottas och de åsikter som framförs som svar på samråden.[1]

Enligt kommitténs bedömning kommer det i normalfallet vara en förutsättning för en välavvägd uppförandekod, att de registrerade hörts och att deras synpunkter har beaktats. Det förefaller både naturligt och nödvändigt att i ett tidigt skede involvera sammanslutningar och organisationer som representerar de registrerade, som exempelvis hyresgästföreningar, konsumentföreningar och arbetstagarorgansationer. Så har man arbetat när man tagit fram flera i dag befintliga branschöverenskommelser. Att inhämta och beakta de registrerades synpunkter kan därmed sägas utgöra god sed för framtagandet av sådana överenskommelser och bör även ske i arbetet med uppförandekoder.

4.1.4 Godkännande av uppförandekod

Enligt dataskyddsförordningen ska sammanslutningar och andra organ som avser att utarbeta en uppförandekod eller ändra eller utöka befintliga uppförandekoder, lämna in utkastet till den behöriga tillsynsmyndigheten. Tillsynsmyndigheten ska yttra sig om utkastet överensstämmer med förordningen och godkänna det om den finner att tillräckliga garantier tillhandahålls.

[1] Skäl 99.

Om utkastet till kod godkänns, och om den berörda uppförandekoden inte avser behandling i flera medlemsstater, ska tillsynsmyndigheten registrera och offentliggöra uppförandekoden.

Vid sin prövning av ett utkast till kod, förefaller det lämpligt att tillsynsmyndigheten beaktar i vad mån man har samrått med de registrerade, och tagit hänsyn till det som framkommit i samrådet.

4.1.5 Behandling i flera medlemsstater

Om ett utkast till uppförandekod avser behandling i flera medlemsstater ska den behöriga tillsynsmyndigheten innan den godkänner utkastet till kod, ändring eller utökning, överlämna det till dataskyddsstyrelsen, som ska avge ett yttrande om utkastet är förenligt med förordningen eller tillhandahåller lämpliga garantier.

Om dataskyddsstyrelsen bekräftar att utkastet är förenligt med förordningen eller tillhandahåller lämpliga garantier, ska styrelsen inlämna sitt yttrande till kommissionen.

Kommissionen får, genom genomförandeakter, besluta att den godkända koden, ändringen eller utökningen som getts in till den, har allmän giltighet inom unionen. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

Kommissionen ska se till att de godkända koder om vilka det har beslutats att de har allmän giltighet, offentliggörs på lämpligt sätt.

Styrelsen ska samla alla godkända uppförandekoder, ändringar och utökningar i ett register och offentliggöra dem på lämpligt sätt.

4.1.6 Nyttan med uppförandekoder

Dataskyddsförordningens regler behöver i många fall specificeras och förtydligas, om förordningen ska göra någon verklig skillnad för den personliga integriteten och faktiskt bidra till bättre skydd och större tydlighet för registrerade och personuppgiftsansvariga.

Uppförandekoder kan på ett pedagogiskt sätt anpassas till de befattningshavare i de berörda verksamheterna som i praktiken gör bedömningar och val avseende vilka system och digitala hjälpmedel som faktiskt används i verksamheten.

Jämfört med en uppförandekod är en registerförfattning svårare att anpassa till konkreta situationer. Författningen tar längre tid att

ta fram, och det är också mer omständligt och tidskrävande att komplettera eller ändra författningen när behov för detta uppstår. En uppförandekod har vidare den fördelen att det är de personuppgiftsansvariga som tillsammans utarbetar den och som därmed snabbare kan komma att tillägna sig innehållet, dvs. sprida och använda sig av uppförandekoden.

Enligt dataskyddsförordningen bör sammanslutningar eller andra organ, som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden, uppmuntras att utarbeta uppförandekoder så att tillämpningen av förordningen effektiviseras, med beaktande av särdragen hos den behandling som görs inom vissa sektorer och de särskilda behov som finns inom mikroföretag samt inom små och medelstora företag. I synnerhet skulle man genom sådana uppförandekoder kunna anpassa personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter, med beaktande av den risk som behandlingen sannolikt innebär för fysiska personers rättigheter och friheter.[2]

Enligt dataskyddsförordningen kan vägledning för den personuppgiftsansvariges eller personuppgiftsbiträdets genomförande av lämpliga åtgärder och för påvisande av att behandlingen är förenlig med förordningen, framför allt ges genom godkända uppförandekoder, godkänd certifiering, riktlinjer från styrelsen eller genom anvisningar från ett dataskyddsombud. [3]

Det har dessutom vissa rättsliga verkningar i dataskyddsförordningen att man ansluter sig till en godkänd uppförandekod:

- Tillämpningen av uppförandekoder får användas för att visa att den personuppgiftsansvarige fullgör sina skyldigheter överlag enligt förordningen (artikel 24).
- En uppförandekod får användas av en personuppgiftsansvarig för att visa att denne uppfyller informationssäkerhetskraven i artikel 32.1.
- Ett personuppgiftsbiträdes anslutning till en uppförandekod får användas för att visa att tillräckliga garantier tillhandahålls avseende lämpliga tekniska och organisatoriska åtgärder för att uppfylla kraven i dataskyddsförordningen och säkerställa att den registrerades rättigheter skyddas (artikel 28.5).

[2] Skäl 98.

- Tillämpningen av en godkänd uppförandekod enligt artikel 83 ska beaktas i samband med beslut om administrativa sanktionsavgifter; i frågan om avgift ska påföras och i så fall med vilket belopp. Det får förstås som att det kan innebära en förmildrande omständighet om den personuppgiftsansvarige har följt en godkänd uppförandekod.
- Efterlevnad av godkända uppförandekoder ska på lämpligt sätt beaktas i samband med en konsekvensbedömning avseende dataskydd enligt artikel 35.

4.2 Exempel på uppförandekoder i Sverige och andra länder

4.2.1 Uppförandekodernas detaljeringsgrad

Uppförandekoder kan variera i fråga om omfång och detaljeringsgrad, beroende på vilken sektor som koden omfattar och vilka frågor som behöver klargöras i den.

Exempelvis kan det finnas såväl koder som är relativt omfattande och praktiskt inriktade, som koder som är mer avgränsade till sin omfattning och som tar sikte på bara en eller ett fåtal frågor.

De exempel på befintliga uppförandekoder som ges nedan representerar både sådana som är mer omfattande och sådana som är mer kortfattade.

Även de branschöverenskommelser, koder och riktlinjer för branscherna som finns redan i dag, kommer att behöva ses över i förhållande till dataskyddsförordningen. Dessa kan då komma att ges in till tillsynsmyndigheten, som efter att ha granskat dem kan godkänna dem som uppförandekoder i dataskyddsförordningens mening.

4.2.2 Svenska uppförandekoder om personuppgifter

Det finns ett antal branschöverenskommelser, etiska riktlinjer och standarder som helt eller delvis innehåller regleringar som skulle kunna ges i en uppförandekod i dataskyddsförordningens mening. Några exempel:

- Fastighetsägarna Sverige och SABO (Sveriges Allmännyttiga Bostadsföretag) har i samarbete med Hyresgästföreningen tagit fram en branschöverenskommelse för behandling av personuppgifter, inklusive kameraövervakning, vid uthyrning av bostäder. Datainspektionen har granskat och godkänt överenskommelsen. Syftet med överenskommelsen är att skapa en gemensam god sed för behandlingen av personuppgifter, inklusive kameraövervakning, på bostadshyresmarknaden. I överenskommelsen finns bl.a. konkreta anvisningar på insamling, användning och gallring av uppgifter hos bostadsföretag. Exempelvis anges hur bostadsföretagen får hantera uppgifter om brott, uppgifter om att en bostad är anpassad för personer med funktionsnedsättning, och uppgifter om att anstånd med hyra medgetts av hälsoskäl.
- På initiativ av Swedish Direct Marketing Association (Swedma) har berörda delar av svenskt näringsliv samt frivilliga insamlingsorganisationer tagit fram riktlinjer för direktmarknadsföring. Dessa syftar till att – mot bakgrund av gällande lagstiftning och allmänt omfattade etiska värderingar – närmare ange, dels vad som kan anses vara god sed vid insamling, användning, spridning och annan behandling av personuppgifter för direktmarknadsföringsändamål, dels beskriva det ansvar som företag, organisationer eller någon annan som utför sådan behandling har.[4] I överenskommelsen regleras bland annat varifrån personuppgifter kan samlas in, vilka uppgifter som får samlas in, villkor för behandlingen, information till de registrerade och rättelse av personuppgifter.

[4] *Regler för användning av personuppgifter m.m. vid direktmarknadsföring för försäljnings-, insamlings-, medlemsvärvningsändamål och liknande.* De medverkande i framtagandet överenskommelsen var Annonsörföreningen, Direkthandelsföretagens förening, Frivilligorganisationernas insamlingsråd, Näringslivets delegation för marknadsrätt Industriförbundet, Svenska postorderföreningen, Sveriges reklamförbund, Swedish Direct Marketing Association (Swedma), Tidningsutgivarna, Posten AB, Telia Info Media Partner. Reglerna har godkänts av Datainspektionen.

- För behandling av personuppgifter i inkassoverksamhet finns det en branschöverenskommelse från Sveriges Inkassoorganisation (SIO). Den säger bland annat att bara sådana uppgifter får behandlas, som har betydelse för genomförande av inkassouppdraget. Överenskommelsen har godkänts av Datainspektionen.
- Vidare finns det en branschöverenskommelse för hantering av personuppgifter i samband med skolfotoverksamhet och försäljning av fotografier och skolkataloger. Överenskommelsen är framtagen av Sveriges Elevfotografers Riksförbund och godkänd av Datainspektionen. Enligt överenskommelsen ska som huvudregel gälla att personuppgifter endast får behandlas om samtycke lämnats av både målsman och den elev som avses med personuppgiften och som kan samtycka.
- Engaging Privacy är ett initiativ för aktörer inom it-branschen i Sverige som vill vara mer proaktiva i frågor som rör integritet och datadriven innovation.[5] Värd för satsningen är RISE/SICS, och de nuvarande medlemmarna är Internetstiftelsen i Sverige, Microsoft, Samsung och TeliaSonera. Ett mål med initiativet är att utveckla en branschgemensam uppförandekod.

4.2.3 Exempel på uppförandekoder om annat än personuppgifter

För att få ytterligare ledning i frågan om hur en uppförandekod kan utformas, är det även av intresse att granska några befintliga uppörandekoder som reglerar annat än personuppgiftsbehandling. Några exempel:

- Det finns en omfattande svensk standard för kvalitet i omsorg, service, omvårdnad och rehabilitering för äldre med omfattande behov i ordinärt och särskilt boende.[6] Standarden utgår från samt strukturerar och konkretiserar innehållet i nu gällande lagar, förordningar och föreskrifter samt riktlinjer, vägledningar, kunskapsstöd och liknande dokument av normerande karaktär. Ett grundläggande användningsområde för standarden är att den som bedri-

[5] www.engagingprivacy.se/ den 11 april 2017.
[6] Svensk standard SS 872500:2015.

ver verksamhet utifrån denna standard kan planera, leda och genomföra samt systematiskt utvärdera och förbättra verksamheten. Inför upphandling av utförare kan kommunen använda standarden som upphandlingsunderlag och därmed även som ett stöd vid uppföljning. Standarden är också tänkt att kunna användas som underlag vid utbildning och kompetensutveckling av personal inom omsorg, service, omvårdnad och rehabilitering av äldre.

- Vidare finns det en kod för medlemsföretagen i Sveriges Byggindustrier. Koden innebär att medlemsföretag och dess medarbetare ska följa lagar och föreskrifter samt verka för sund konkurrens och tidsenliga relationer såväl inom företaget som i förhållande till kunder och leverantörer. I koden anges bland annat att medlemsföretag ska föra korrekt redovisning av ekonomiska transaktioner samt motverka svartarbete, övrig ekonomisk brottslighet och påverkan från illegal verksamhet, att medlemsföretagen ska agera korrekt och inte bjuda på, eller anordna resor, ge gåvor eller andra tjänster eller förmåner som inte kan granskas och redovisas öppet. Uppförandekoden utgör ett av kriterierna för medlemskap i Sveriges Byggindustrier. Avsteg från eller underlåtelse att agera och korrigera avsteg från koden kan, som yttersta konsekvens, utgöra grund för uteslutning. Till koden finns det faktablad och vägledande kommentarer. Det är möjligt för medlemmarna att signera uppförandekoden.
- Konsumentverket har ingått flera branschöverenskommelser med aktörer inom olika branscher. Exempelvis har Konsumentverket och mobiloperatörerna Telenor Sverige AB, TeliaSonera Sverige AB, Hi3G Access AB, Tele2 Sverige AB samt Netett Sverige AB, träffat en överenskommelse om marknadsföring av täckning för mobila tjänster. I överenskommelsen regleras bl.a. vilken information som konsumenten ska få om täckning.[7]

[7] Konsumentverkets branschöverenskommelse BÖ 2014:02.

4.2.4 Exempel i andra länder på uppförandekoder om personuppgifter

I andra länder har vissa branscher kommit mycket långt i att ta fram uppförandekoder för hur personuppgifter ska hanteras. Några exempel:

- I Norge finns den s.k. *Normen* som är ett slags uppförandekod med en norm för informationssäkerhet för vård- och omsorgssektorn. Normen är en sammanställning av lagstiftningens krav på informationssäkerhet, men ställer ibland också strängare krav. Det innebär att Normen ställer krav som specificerar och kompletterar gällande regelverk. Normen behandlas utförligare i kapitlet om Hälso- och sjukvård och välfärdsteknik inom socialtjänsten.
- I Storbritannien har dataskyddsmyndigheten ICO (Information Commissioner's Office) tagit fram en uppförandekod (eng. code of practice) för information till registrerade, transparens och kontroll. I uppförandekoden lämnas rekommendationer om vad som bör ingå i informationen samt hur och när den bör lämnas till de registrerade.[8]
- I Tyskland har försäkringsbolagens branschorganisation, Gesamtverband der Deutschen Versicherungswirtschaft, tagit fram en uppförandekod för hantering av personuppgifter. I koden regleras bl.a. hur uppgifter får samlas in och användas.[9]
- I Nederländerna har det tagits fram en uppförandekod för hur finansiella institutioner (banker och försäkringsbolag) ska hantera personuppgifter.[10] Uppförandekoden har utarbetats av Nederländska bankföreningen (Nederlandse Vereniging van Banken) och Nederländska försäkringsföreningen (Verbond van Verzekeraars). Den har därefter (i april 2010) godkänts av den nederländska dataskyddsmyndigheten (College Bescherming Persoonsgegevens). Syftet med koden är att på ett korrekt sätt förtydliga

[8] ICO:s kod *Privacy notices, transparency and control*
[9] Gesamtverband der Deutschen Versicherungswirtschaft, *Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft*.
[10] Code of Conduct for the Processing of Personal Data by Financial Institutions.

hur den nederländska dataskyddslagstiftningen ska tillämpas inom bank- och försäkringssektorn.

- På europeisk nivå har CISPE (Cloud Infrastructure Services Providers in Europe som är en sammanslutning av leverantörer av molntjänster för infrastruktur) tagit fram en uppförandekod för molntjänster för infrastruktur.[11] Ett angivet syfte med koden är att när en leverantör förklarar att den följer koden, ska kunderna kunna känna sig säkra på att de kan använda leverantörens tjänster för att hantera personuppgifter på ett sätt som är förenligt med EU:s dataskyddsbestämmelser. Det framgår inte om koden är granskad eller godkänd av någon dataskyddsmyndighet.

4.3 Statliga myndigheters roller och resurser i arbetet med uppförandekoder

Även om utarbetandet av förslag till uppförandekoder ska utföras av de personuppgiftsansvarigas eller personuppgiftsbiträdenas branschorganisationer, kommer arbetet med att uppmuntra, granska och godkänna uppförandekoder att behöva göras av nationella myndigheter och EU-gemensamma organ.

Kommittén föreslår (se exempelvis kapitel 5 och 6) att regeringen så långt som möjligt uppdrar åt vissa utpekade myndigheter att i samråd med Datainspektionen stå för merparten av det arbete som en myndighet behöver utföra när det gäller uppförandekoder. Skyldigheten att uppmuntra framtagandet av koder ligger enligt dataskyddsförordningen både på medlemsstaten och på tillsynsmyndigheten (artikel 40.1 i dataskyddsförordningen). Det kan i sammanhanget finnas anledning att beakta regeringens möjligheter att ge uppdrag till Datainspektionen. Dessa möjligheter kommer ju att vara begränsade enligt artikel 52 i dataskyddsförordningen. Det är även viktigt att se till att Datainspektionen inte ska bli överbelastad med uppdrag av detta slag inom en rad olika områden samtidigt. Slutligen är det många gånger den branschspecifika myndigheten som bäst känner till parterna inom den aktuella sektorn och de vanligast förekommande integritetsrelaterade frågorna och problemen. En del branschspecifika

[11] *Data Protection Code of Conduct for Cloud Infrastructure Service Providers*, CISPE, 27 January 2017.

myndigheter har dessutom erfarenhet av att samla parterna inom vissa branscher för att diskutera regelverkets utformning på exempelvis föreskriftsnivå.

Det kan således vara lämpligt att en annan myndighet än Datainspektionen samlar branschen till ett första möte där möjligheten till uppförandekod diskuteras. Likaså kan en annan myndighet än Datainspektionen vid behov hålla samman arbetet fram till dess att koden ska godkännas.

Datainspektionen roll bör inskränkas till det som ingen annan myndighet kan eller får göra, det vill säga att fatta det slutliga beslutet att godkänna koden. I de olika områdesavsnitten i detta betänkande, ger vi konkreta förslag till vilka andra myndigheter som bör involveras i arbetet med uppförandekoder: Skolverket, Konsumentverket, Arbetsmiljöverket och eventuellt E-hälsomyndigheten. Vidare föreslås i betänkandet *digitalforvaltning.nu*[12] att den myndighet som får det samlade ansvaret för digitaliseringen av offentlig sektor, ska få i uppdrag att stödja myndigheter i utarbetandet av gemensamma uppförandekoder i dataskyddsförordningens mening.

Arbetet med att initiera och stödja framtagandet av uppförandekoder förutsätter viss kompetens i att hantera projekt av liknande art. Det finns emellertid specialister på detta som kan anlitas av myndigheterna för att leda och genomföra sådana projekt, exempelvis inom SIS (Swedish Standards Institute). En möjlighet är även att myndigheterna låter utföra arbetet genom SIS. Flera av de myndigheter som kommittén föreslår ska få särskilda uppdrag och resurser för att initiera och stödja framtagandet av uppförandekoder, är redan i dag medlemmar i SIS (exempelvis Skolverket, Arbetsmiljöverket och Konsumentverket). Om flera myndigheter väljer att utföra arbetet genom SIS, kan det också innebära effektivitetsvinster genom att SIS då kan samordna arbetet och dra nytta av tillvägagångssätt och metoder inom flera olika branscher. Även om SIS involveras, innebär den statliga finansiering som kommittén föreslår, att medverkan i arbetet med att utarbeta koderna kommer att vara kostnadsfritt för de sammanslutningar av personuppgiftsansvariga eller personuppgiftsbiträden som aktualiseras. Den resulterande uppförandekoden

[12] Utredningens om effektiv styrning av nationella digitala tjänster betänkande *digitalforvaltning.nu* (SOU 2017:23).

kommer efter Datainspektionens godkännande att offentliggöras och därmed vara fritt tillgänglig utan någon kostnad (artikel 40.6).

Vår bedömning är att varken Datainspektionen eller någon av de andra myndigheterna nödvändigtvis behöver rekrytera särskild personal för arbetet med uppförandekoder. Myndigheterna kommer dock att behöva använda resurser åt arbetet med uppförandekoder. De kommer därför att behöva ökade anslag under tiden då arbetet med att utarbeta uppförandekoden pågår.

DEL III

Integritetskommitténs förslag

5 Skolan

5.1 Riskerna

Som framgår av kommitténs delbetänkande, har skolornas huvudmän att hantera ett antal risker för den personliga integriteten, relaterade till:

- Digitala lärplattformar och digitala läromedel (allvarlig risk)
- Sociala medier i undervisningen (allvarlig risk)
- Elevhälsan (viss risk)
- Skolfederationen (viss risk)
- Kameraövervakning inomhus i skolor (påtaglig risk).

5.2 Förslag till åtgärder

5.2.1 Uppförandekod

Integritetskommitténs förslag: Regeringen bör ge Skolverket i uppdrag att initiera och stödja utarbetandet av en uppförandekod för skolan.[1]

[1] Med skola avses här sådan verksamhet som i 1 kap. 1 § skollagen (2010:800) går under beteckningen skolväsendet.

Ett allmänt hållet regelverk

Det finns inget särskilt regelverk för hur personuppgifter ska hanteras i skolan, utöver personuppgiftslagen (fr.o.m. 25 maj 2018 dataskyddsförordningen samt de eventuella, kompletterande regler som Utbildningsdatautredningen kan komma att föreslå, se nedan). Det finns samtidigt ett stort behov av kunskap om hur det allmänt hållna regelverket ska tillämpas på skolområdet.

En särskild registerförfattning för skolan skulle sannolikt bidra till en bättre tydlighet än både dagens generella bestämmelser i personuppgiftslagen och den kommande dataskyddsförordningen, som även den är relativt allmänt hållen.

Utbildningsdatautredningen[2] ska lämna sitt slutbetänkande ungefär samtidigt som Integritetskommittén. Utbildningsdatautredningen har haft i uppdrag att undersöka bland annat vilken reglering av personuppgiftsbehandling inom utbildningsområdet som är möjlig och kan behövas utöver dataskyddsförordningen och den generella reglering som Dataskyddsutredningen kommer att föreslå. Integritetskommittén och Utbildningsdatautredningen har löpande stämt av med varandra vilka frågor och förslag som varit aktuella för respektive utredning.

Författning eller uppförandekod

Ett alternativ till särskild registerförfattning på skolområdet, kan vara en uppförandekod (se kapitel 4 om uppförandekoder). En fördel med en uppförandekod är att den på ett pedagogiskt sätt kan utformas så att den riktar sig till de befattningshavare i skolorna som i praktiken gör bedömningar och val av vilka digitala hjälpmedel som faktiskt används i skolan.

En registerförfattning är, jämfört med en uppförandekod, svårare att utforma så att den ger ledning i konkreta situationer. En författning tar också längre tid att ta fram. Det är också mer omständligt och tidskrävande att komplettera eller ändra en författning när behov för detta uppstår i framtiden.

En uppförandekod har vidare den fördelen att det är de personuppgiftsansvariga, dvs. i detta fall skolhuvudmännen, som tillsam-

[2] U 2016:03, dir. 2016:63.

mans utarbetar koden. De kan därmed förväntas snabbare komma att tillägna sig innehållet, dvs. sprida och använda sig av uppförandekoden, än vad som skulle vara fallet med en helt ny lag.

I kapitel 4 om uppförandekoder, beskrivs olika typer av uppförandekoder. Mot bakgrund av de risker som vi lyfter fram i delbetänkandet, anser kommittén att skolan är exempel på en verksamhet som kan behöva en mer omfattande kod, som hanterar ett flertal olika frågor.

Branschorganisationer för skolan

På skolområdet finns det tydliga och välorganiserade sammanslutningar som företräder kategorier av personuppgiftsansvariga, vilka skulle kunna vara upphovsmän till en uppförandekod: de största på området är Sveriges kommuner och landsting (SKL) och Friskolornas riksförbund.

Frågor som kan tas upp i en uppförandekod för skolan

Med utgångspunkt i dels de risker som kommittén har bedömt föreligger på skolområdet, dels de skyldigheter som kommer att åligga skolorna enligt dataskyddsförordningen, kan en uppförandekod för skolan beröra bland annat följande frågor:

- Hur skolorna ska gå till väga för att uppfylla kravet i artikel 30 i dataskyddsförordningen på register över vilka behandlingar av personuppgifter som görs i skolan. Lämpligtvis innefattar koden en metod eller mall (med exempel) för praktisk inventering och dokumentation av vilka uppgifter om eleverna som hanteras i de lärplattformar och digitala läromedel som används på skolan, och om hur uppgifterna används (både av skolan och av leverantören).
- Hur skolans huvudman och skolans ledning ska bestämma och föra en förteckning över vilka sociala medier som ska användas i undervisningen eller i annan kommunikation med elever och vårdnadshavare.
- Hur konsekvensbedömningar avseende dataskydd (artikel 35 i dataskyddsförordningen) ska genomföras före införandet av varje nytt system eller större ändring i befintliga system. Det kan röra

sig om att skolan börjar använda en ny lärplattform, ett nytt digitalt läromedel eller ett nytt socialt nätverk. Det kan också röra sig om ändrade användarvillkor för tjänster som skolan redan använder sig av. Koden bör även innefatta en mall eller exempel för hur en konsekvensbedömning kan genomföras i praktiken.

- Hur inbyggt dataskydd och dataskydd som standard (artikel 25 i dataskyddsförordningen) ska genomföras, med angivande av exempel.
- I vilka situationer som behandlingen kan bygga på samtycke från eleven eller vårdnadshavarna. Det bör exempelvis anges att tystnad, på förhand ikryssade rutor eller inaktivitet inte ska utgöra ett giltigt samtycke.[3] Vidare kan anges att samtycke inte ska betraktas som frivilligt om eleven inte har någon genuin eller fri valmöjlighet eller inte utan problem kan vägra eller ta tillbaka sitt samtycke.[4]
- Exempel på rutiner och riktlinjer för hur skyddade personuppgifter ska hanteras. Exempelvis bör anges att det klart och tydligt måste framgå att personuppgifter är skyddade, till exempel genom flaggning, och att det inte ska råda någon som helst oklarhet om att det är uppgifter som särskilt behöver skyddas.[5]
- Hur och när uppgifter ska gallras. Uppgifter om inloggningar och arbetssätt i lärplattformar eller digitala läromedel bör exempelvis kunna gallras eller avidentifieras tämligen omgående, medan betyg och andra författningsreglerade dokumenttyper som individuella åtgärdsprogram och utvecklingsplaner behöver sparas under längre tid. För kommuner bör även beskrivas när uppgifter i skolans it-system ska omfattas av en dokumenthanteringsplan.
- Exempel på informationssäkerhetsåtgärder som en skola behöver vidta för att uppfylla kraven i artikel 32 i dataskyddsförordningen (avseende exempelvis behörighet, loggning, säkerhet vid åtkomst över internet osv).

[3] Se skäl 32 i dataskyddsförordningen.
[4] Se skäl 42 i dataskyddsförordningen.
[5] Se Datainspektionens *Checklista för skolor – Skyddade personuppgifter i skolan* (december 2012).

- Under vilka omständigheter information kan delas mellan skolhälsovården och den undervisande verksamheten (rekommendationen bör ges efter samråd med Socialstyrelsen).
- Vilken information som måste ges till elever, vårdnadshavare och anställda vid skolan om hur uppgifter används, med angivande av exempel. Här bör exempelvis anges hur information kan ges med hjälp av standardiserade symboler för att ge en överskådlig, begriplig, lättläst och meningsfull överblick över hur uppgifterna hanteras och av vem.[6]
- Rutiner och riktlinjer för hur stora datauttag (det kan exempelvis röra sig om många uppgifter om en elev, eller om ett fåtal slags uppgifter om ett stort antal elever) från systemen bör bedömas. Exempelvis bör anges hur tryckfrihetsförordningens bestämmelser kan bli tillämpliga på loggar i lärplattformar, digitala läromedel och sociala medier. Vidare bör anges när och hur 21 kap. 7 § offentlighets- och sekretesslagen (2009:400) kan bli tillämplig.
- I vilka situationer kameraövervakning inomhus kan användas och hur skolan bäst kan uppfylla kraven i kameraövervakningslagen på exempelvis dokumentation och information. Exempelvis bör anges att kameraövervakning inte är en lösning som ska väljas i första hand. Här kan det anges vilka alternativ till kameraövervakning som kan finnas, som exempelvis inlåsning av särskilt värdefull utrustning, förstärkt skalskydd till vissa rum och utrymmen i skolan, ombyggnationer av ytor med skymd sikt, rörelsestyrda vattenkranar, ökad vuxennärvaro etc.[7]

Vem ska uppmuntra utarbetandet av uppförandekoder?

Skyldigheten att uppmuntra utarbetandet av uppförandekoder enligt artikel 40 i dataskyddsförordningen gäller inte bara Datainspektionen. Regeringen kan och bör agera även genom andra myndigheter.

[6] Se skäl 60 i dataskyddsförordningen.
[7] Se Datainspektionens checklista *Kameraövervakning inomhus i skolor* (augusti 2015). Förslag om kameraövervakning kommer att lämnas av Utredningen om kameraövervakning – brottsbekämpning och integritetsskydd (Ju 2015:14) som bl.a. ska ta ställning till om integritetsskyddet i samband med kameraövervakning i skolor behöver förbättras.

Som framgår i avsnittet om uppförandekoder, anser Integritetskommittén att regeringen så långt som möjligt bör uppdra åt andra myndigheter att i samråd med Datainspektionen stå för merparten av det arbete som en myndighet behöver utföra när det gäller uppförandekoder. Ett skäl till detta är att Datainspektionen inte ska bli överbelastad med uppdrag av detta slag inom en rad olika områden på en gång, samtidigt som myndigheten har ett stort arbete framför sig med att anpassa sin verksamhet till dataskyddsförordningen. Ett annat skäl till detta är att en branschspecifik myndighet bättre än Datainspektionen känner till vilken slags vägledning (både till form och innehåll) som efterfrågas inom branschen samtidigt som myndigheten inte sällan redan har etablerade kontakter med aktörer och branschföreträdare.

Det sagda gäller i hög grad för Skolverket som under de senaste åren samlat på sig och vidareförmedlat kunskap och erfarenheter gällande skolans digitalisering.

Ordet ”uppmuntra” används i dataskyddsförordningen, och ska enligt kommitténs tolkning i detta sammanhang närmast förstås som att initiera och stödja. I arbetet med att initiera och stödja framtagandet av uppförandekoder, kan Skolverket exempelvis bjuda in branschorganisationerna och andra ansvariga myndigheter för ett samtal om förutsättningarna för en uppförandekod på området, där även alternativen till en uppförandekod kan tas upp.

Om det inte finns en uppförandekod, måste de personuppgiftsansvariga och personuppgiftsbiträdena själva – utan närmare tolkningshjälp – tillämpa dataskyddsförordningen eller annan, allmänt hållen ramlagstiftning. Det skulle kunna innebära en ökad risk för administrativa sanktionsavgifter enligt artikel 83 i dataskyddsförordningen.

Det krävs en särskild kompetens för att leda projekt för att ta fram uppförandekoder. Det finns specialister på detta som kan anlitas av myndigheterna för att leda och genomföra sådana projekt, exempelvis inom SIS (Swedish Standards Institute). Särskilt för Skolverkets del skulle det kunna vara ett alternativ att utföra allt eller en del av arbetet med hjälp av SIS, eftersom Skolverket är medlem i SIS.

Sammanfattningsvis anser vi att regeringen bör ge Skolverket i uppdrag att i samråd med Datainspektionen vidta åtgärder för att initiera och stödja utarbetandet av en uppförandekod för skolan.

5.2.2 Sekretess

Integritetskommitténs förslag: Regeringen bör låta utreda frågan om ett utökat sekretsskydd för uppgifter om elever i skolans it-system.

I delbetänkandet konstaterade kommittén att det genereras allt fler och allt mer detaljerade uppgifter om eleverna i skolan, alltifrån hur de använder sig av läromedel och chattar med klasskamraterna, till vilka kamrater de helst syns tillsammans med i skolan. Kommittén konstaterade också att det för elever i grundskolan och gymnasieskolan inte finns någon sekretess eller tystnadsplikt för större delen av den växande uppgiftsmassan.

Tidigare utredningar

Utredningen om offentlighet och sekretess i skolan konstaterade att nya arbetsformer inom skolan, som bl.a. innebar ökade dokumentationskrav för uppföljning och utvärdering av arbetet och insatserna inom elevhälsan, sannolikt medförde att allt fler känsliga uppgifter om elever skulle komma att hanteras av personalen.[8] Man beaktade också att införandet av arbetsmetoder med mer individualiserad undervisning skulle leda till ökad dokumentation om eleverna. Utredningens kartläggning av dokumentationen i skolorna och analysen av dokumentens offentligrättsliga status, visade emellertid inte på sådana problem eller brister i sekretessregleringen att det borde föranleda nya eller ändrade bestämmelser. Behovet av ett sekretesskydd för elevarbeten behandlades särskilt. Det ansågs att uppgifter som inte omfattades av sekretess eftersom de var direkt hänförliga till undervisningen även fortsättningsvis borde vara offentliga. Det kunde finnas behov av att i undantagsfall sekretessbelägga annars offentliga uppgifter, t.ex. när uppgifterna avslöjade känsliga personliga förhållanden eller när det av annan orsak kunde förväntas att en enskild elev skulle ta mycket illa vid sig om uppgifterna spreds. Eftersom stor restriktivitet borde iakttas när man övervägde att införa nya sekre-

[8] Utredningens om offentlighet och sekretess i skolan betänkande *Sekretess i elevernas intresse – Dokumentation, samverkan och integritet i skolan* (SOU 2003:103), s. 120 ff.

tessbestämmelser som begränsade offentligheten i myndigheternas verksamhet och avsaknaden av en sådan bestämmelse inte heller påtalats som ett praktiskt problem, föreslogs ingen ändring.

Integritetsskyddskommittén ansåg att det från integritetsskyddssynpunkt var en riskfaktor att dokumentationen om enskilda elever liksom tillgängligheten till denna dokumentation ökade i den ordinarie undervisningen.[9] Det ifrågasattes mot denna bakgrund om skolsekretessens avgränsning till uppgifter i den elevvårdande verksamheten var ändamålsenlig.

Utredningen om sekretess för uppgifter i skolväsendet och vissa andra utbildningsformer lämnade betänkandet *Skolans dokument – insyn och sekretess*.[10] Utredningen behandlade bland annat behovet av en möjlighet till sekretess för uppsatser och andra elevarbeten. När det gäller behovet av skydd för uppgifter i elevarbeten konstaterade utredningen följande. Elevarbeten ingår i underlaget för betygssättningen. I de samrådskontakter som utredningen hade haft, hade det inte framkommit att avsaknaden av ett sekretesskydd för elevarbeten var ett praktiskt problem, bland annat eftersom elevarbeten ofta lämnades tillbaka till eleverna efter en bedömning. Kvar står dock att elevarbeten bör hanteras i enlighet med de krav som ställs för hantering av allmänna handlingar.

Utredningen konstaterade också att uppgifter i en uppsats eller ett elevarbete av annat slag, med gällande regler normalt sett är att betrakta som offentliga. Undantagsvis kan de omfattas av sekretessen i den särskilda elevstödjande verksamheten. Så kan vara fallet om uppgifterna föranleder åtgärder som faller inom den särskilda elevstödjande verksamheten. Uppgifter om enskildas hälsa och sexualliv som finns i elevarbeten kan enligt utredningen omfattas av sekretess enligt 21 kap. 1 § offentlighets- och sekretesslagen.

Utredningen menade att insynsintresset beträffande hur utbildningsväsendet fungerar är betydande. Ett minimikrav som ställts har varit att uppgifter som uteslutande rör elevernas studieresultat alltid ska vara offentliga. De frågor som ingår i skolans värdegrundsuppdrag kan i andra sammanhang anses falla inom den privata sfären. Att de finns i ett utbildningssammanhang skiljer det dock från dessa

[9] Integritetsskyddskommitténs delbetänkande, *Skyddet för den personliga integriteten – Kartläggning och analys* (SOU 2007:22), s. 34.
[10] SOU 2011:58.

andra situationer. Intresset av insyn får anses stort också i den del av skolans uppdrag som avser värdegrundsarbetet. Elevarbeten ingår i det underlag på vilket betyg ska sättas och rättssäkerhetsskäl talar därför också för en öppenhet, enligt utredningen.

Ett generellt skydd för uppgifter av det aktuella slaget skulle enligt utredningen kunna uppnås genom en regel om generell sekretess inom skolväsendet utanför den särskilda elevstödjande verksamheten med ett rakt skaderekvisit för uppgifter om enskildas personliga förhållanden.

Utredningen kom fram till att insynsintresset beträffande skolväsendets sätt att fungera är betydande, och att elevarbeten ingår i det underlag på vilket betyg ska sättas samt att även rättssäkerhetsskäl talar för öppenhet. Enligt utredningens bedömning fanns därmed inte tillräckliga skäl att genom ny eller ändrad lagstiftning utöka sekretessen att omfatta också uppgifter i elevarbeten.

Ännu har inga av de förslag som utredningen lämnade genomförts.

Datainspektionen har i remissvar påpekat att det inom skolundervisningen i stort tenderar att förekomma mer och mer uppgifter om elevernas personliga åsikter, tankar och förmågor. Det är enligt Datainspektionen ur ett integritetsperspektiv inte acceptabelt att sådana uppgifter helt kan sakna sekretesskydd.[11]

Utredningen om offentlighetsprincipen i fristående skolor har i betänkandet *Ökad insyn i fristående skolor* föreslagit att offentlighetsprincipen ska införas hos huvudmän för fristående skolor.[12] En ny bestämmelse föreslås i offentlighets- och sekretesslagen av innebörd att vad som föreskrivs i tryckfrihetsförordningen om rätt att ta del av allmänna handlingar hos myndigheter i tillämpliga delar ska gälla också handlingar hos huvudmän för fristående skolor. Samtliga huvudmän för fristående skolor ska omfattas. Huvudmännen ska vid tillämpningen av offentlighets- och sekretesslagen jämställas med myndigheter.

[11] Datainspektionens remissvar på betänkandet *Skolans dokument – insyn och sekretess* (SOU 2011:58), Datainspektionens dnr 1502-2011.
[12] SOU 2015:82.

Integritetskommitténs bedömning

Tidigare utredningar tillkom i en tid då digitaliseringen av skolan ännu inte hade nått lika långt som i dag. Nu har lärplattformar och digitala läromedel utvecklats och fått en större spridning än tidigare. Vidare synes tidigare utredningar ha tagit fasta på de olika dokumenttyper som skapas i samband med handläggningen av ärenden hos skolorna, eller på uppgifter som finns i andra, avgränsade dokumenttyper som exempelvis uppsatser. Beträffande uppsatserna var exempelvis uppfattningen att uppsatserna lämnas tillbaka till eleverna, vilket sannolikt kommer att göras i allt mindre omfattning när elevarbeten i stället lämnas in och därefter sparas elektroniskt.

Det innebär att effekterna av den omfattande digitaliseringsvågen i allt väsentligt inte har beaktats i de tidigare utredningarna. Om digitaliseringen tas med i beaktande, blir bilden enligt kommitténs mening en helt annan. I dagens digitaliserade skola kan det hanteras ett stort antal olikartade och närgångna uppgifter om varje enskild elev. Dessa uppgifter skapas inte medvetet i och med att viss dokumentation upprättas, utan genereras automatiskt, och många gånger omedvetet, genom att eleverna använder olika former av it-stöd i skolan.

Som vi konstaterade i delbetänkandet finns det ett stort intresse hos olika aktörer i samhället att kunna använda sig av dessa uppgiftssamlingar för olika ändamål. Mycket tyder på att kunskapen om hur dessa datamängder faktiskt ska kunna utnyttjas ännu är under utveckling, men att vi framöver kommer att få se en vilja att få åtkomst till data hos skolorna, ner på individnivå.

Kommittén anser liksom tidigare utredningar att det är viktigt att det finns insyn i skolornas verksamhet, och att en förutsättning för detta är att det är möjligt att ta del av vissa uppgifter om enskilda elever. Vi menar också att tillgängliggörandet och vidareanvändningen av data från skolornas system bör uppmuntras, när data efterfrågas och används av privata och offentliga aktörer som vill utveckla nya system och undervisningsmetoder.

Med tanke på ökningen av uppgifter om eleverna som behandlas i och med att skolan digitaliseras, finns det emellertid anledning att befara att stora och närgångna uppgiftsmängder om eleverna på individnivå kommer att lämnas ut, eftersom de inte omfattas av någon sekretessregel. Ett utökat sekretesskydd för personuppgifter

i skolan skulle kunna förbättra skyddet, utan att för den skull försämra förutsättningarna för utomstående att granska skolornas verksamhet.

Kommittén anser därför att regeringen bör låta utreda frågan om ett utökat sekretsskydd för uppgifter om elever i skolans it-system.

5.2.3 Statlig kontroll och styrning

Integritetskommitténs förslag: Regeringen bör ge Skolinspektionen och Datainspektionen i uppdrag att hitta lämpliga samarbetsformer.

Kommittén anser att de ansvariga myndigheterna på området, i första hand Datainspektionen, Skolverket och Skolinspektionen bör utveckla sin samverkan när det gäller tillsyn och vägledning till skolorna i ärenden och frågor som rör skolornas digitalisering.

Skolinspektionen har en mycket omfattande och djupgående tillsynsverksamhet. Datainspektionens tillsyn av skolorna är av naturliga skäl av en helt annan och mindre omfattning.

Samverkan mellan Skolinspektionen och Datainspektionen kan exempelvis bestå i att Skolinspektionen, om myndigheten i sin tillsyn uppmärksammar ett återkommande problem för skolorna som rör behandling av personuppgifter, underrättar Datainspektionen om detta. Datainspektionen kan då genom vägledning eller tillsyn vidta åtgärder för att bidra till att avhjälpa problemen. Myndigheternas samarbete bör utformas på ett sätt som hjälper dem att hitta och motverka problem i skolorna. Samarbetet bör också vara anpassat till skolornas och myndigheternas aktuella behov. Ett möjligt exempel på samverkan skull kunna vara att Skolinspektionen i sin tillsyn uppmärksammar en ökning i användningen av kameraövervakning inomhus i skolor i ett visst geografiskt område. Myndigheten skulle då kunna meddela Datainspektionen om ökningen, varpå Datainspektionen skulle kunna rikta informationsinsatser om kameraövervakning till skolorna i området.

I arbetet med att initiera och stödja och granska en uppförandekod för skolan, kommer enligt vårt förslag Datainspektionen och Skolverket att behöva samverka. Därutöver är det viktigt att Skolinspektionen och Datainspektionen också utvecklar ett samarbete.

Regeringen bör därför ge Skolinspektionen och Datainspektionen i uppdrag att hitta lämpliga samarbetsformer.

6 Arbetslivet

6.1 Riskerna

Som framgår av kommitténs delbetänkande, finns det inom arbetslivet ett antal risker för den personliga integriteten för arbetstagare, relaterade till:

- Användningen av positionering och annan övervakning för att kontrollera arbetstagarnas aktiviteter och beteenden på arbetet (allvarlig risk)
- Företeelsen att arbetsgivare skannar av sociala medier för att bilda sig en uppfattning om vad arbetstagarna gör på nätet (viss risk)
- Kompetensdatabaser och utförande av bakgrundskontroller (viss risk)
- Kameraövervakning på arbetsplatser (allvarlig risk)
- Företeelsen att vårdgivare tillhandahåller såväl hälso- och sjukvård som personaladministrativa tjänster (viss risk).

6.2 Förslag till åtgärder

Integritetskommitténs förslag: Regeringen bör ge Arbetsmiljöverket i uppdrag att initiera och stödja utarbetandet av uppförandekoder för arbetslivet.

Ett allmänt hållet regelverk

Det finns inget särskilt regelverk för hur personuppgifter ska hanteras i förhållandet mellan arbetsgivare och arbetstagare, utöver personuppgiftslagen och, fr.o.m. 25 maj 2018, dataskyddsförordningen. Det finns samtidigt ett stort behov av kunskap om hur det allmänt hållna regelverket ska tillämpas inom arbetslivet.

En särskild registerförfattning för personlig integritet i arbetslivet skulle, i alla fall i teorin, kunna bidra till en bättre tydlighet än både dagens generella bestämmelser i personuppgiftslagen och den kommande dataskyddsförordningen, som även den är relativt allmänt hållen. I praktiken har det dock visat sig vara svårt att ta fram en lagtext som är både acceptabel för arbetslivets parter och som förtydligar rättsläget.

Det pågår för närvarande en utredning inom Arbetsmarknadsdepartementet som har till uppgift att se över och föreslå anpassningar till dataskyddsförordningen av författningar som departementet förfogar över. Utredaren ska emellertid inte utreda eller överväga förstärkningar av den personliga integriteten i arbetslivet utöver sådana förstärkningar som direkt följer av dataskyddsförordningen. Utredningsuppdraget ska slutrapporteras senast den 31 maj 2017.[1]

Lagförslag i tidigare utredningar

Integritetsskyddet i arbetslivet har varit föremål för tre olika utredningar sedan år 2002. Alla tre har konstaterat brister i integritetsskyddet för arbetstagare och föreslagit ändringar och förtydliganden i regelverket. Hittills har dock inget av förslagen lett till lagstiftning. Det senaste mest omfattande förslaget lämnades av Utredningen om integritetsskydd i arbetslivet i betänkandet *Integritetsskydd i arbetslivet*.[2] Förslaget fick under remissbehandlingen omfattande kritik, bl.a. avseende nyttan med en så allmänt hållen reglering som den som föreslogs. Det bör samtidigt noteras att förslagen välkomnades av vissa instanser. Även några remissinstanser som i princip välkomnade en reglering på området, ansåg emellertid att förslaget var så

[1] Regeringskanslibeslut 2016-06-10 (A2016/01274/SV).
[2] SOU 2009:44.

otydligt att det inte skulle bidra till ökad klarhet på området. Andra instanser motsatte sig reglering av området av principiella skäl. Enligt uppgift behandlas betänkandet inte längre aktivt i Regeringskansliet.

Frågan om registerutdrag i arbetslivet har därefter givits en separat och fördjupad analys av Utredningen om registerutdrag i arbetslivet. I betänkandet *Registerutdrag i arbetslivet*[3] föreslog utredningen att det ska vara förbjudet för arbetsgivare att utan författningsstöd begära att en arbetssökande ska visa upp eller överlämna ett utdrag ur belastningsregistret. Betänkandet handläggs för närvarande i Regeringskansliet och har nyligen även diskuterats i riksdagen.[4]

Uppförandekoder

En uppförandekod (se kapitel 4 om uppförandekoder) för integritetsskyddet inom arbetslivet, skulle kunna utgöra ett komplement eller ett alternativ till en särskild registerförfattning på arbetslivsområdet.

En fördel med en uppförandekod är att den särskilt kan riktas in på branschspecifika frågeställningar och problem. Den kan också innehålla konkreta råd, anvisningar och exempel, i en utsträckning som inte är möjlig i lagtext.

En uppförandekod har vidare den fördelen att det är de personuppgiftsansvariga, dvs. i detta fall arbetsgivarna, som tillsammans utarbetar koden. De kan därmed förväntas snabbare komma att tillägna sig innehållet, dvs. sprida och använda sig av uppförandekoden, än vad som skulle vara fallet med en helt ny lag.

En registerförfattning är, jämfört med en uppförandekod, svårare att anpassa till konkreta situationer, och författningen tar längre tid att ta fram. Det är också mer omständligt och tidskrävande att komplettera eller ändra en författning när behov för detta uppstår i framtiden. Det har hittills inte heller låtit sig göras att ta fram en lagstiftning för integritetsskydd inom arbetslivet som är godtagbar för arbetslivets olika parter och som innebär ett förtydligande i förhållande till personuppgiftslagens allmänt hållna bestämmelser.

---

[3] SOU 2014:48.

[4] Skriftlig fråga från riksdagsledamoten Jenny Petersson till arbetsmarknads- och etableringsminister Ylva Johansson den 30 november 2016. Se även interpellation 2015/16:48 den 22 oktober 2015 *Saknad proposition* av Jenny Petersson till arbetsmarknadsminister Ylva Johansson.

Mot den beskrivna bakgrunden, anser vi att integritetsskyddet på arbetslivsområdet lämpar sig väl för en uppförandekod.

I kapitlet om uppförandekoder beskrivs olika typer av uppförandekoder. Mot bakgrund av de risker som kommittén lyfter fram i delbetänkandet, anser vi att arbetslivsområdet är exempel på ett område där det kan behövas olika koder för olika branscher, beroende på vilka integritetsrisker som gör sig gällande i respektive bransch. Exempelvis har positionering lyfts som ett problem särskilt inom transportsektorn, kameraövervakning inom restaurang- och cafénäringen, och detaljerad tidmätning inom äldrevården och i call-center-verksamhet.

Branschorganisationer för arbetslivet

På arbetslivsområdet finns det ett flertal tydliga och välorganiserade sammanslutningar som företräder kategorier av personuppgiftsansvariga, vilka skulle kunna vara upphovsmän till uppförandekoder, dvs. de olika arbetsgivarorganisationer som organiserar sig branschvis. De motsvaras av branschbaserade arbetstagarorganisationer.

Arbetstagarorganisationernas medverkan i uppförandekoderna

Som framgår i det allmänna avsnittet om uppförandekoder, bedömer Integritetskommittén att en välavvägd uppförandekod normalt sett bygger på att de registrerade hörts och att deras synpunkter har beaktats.

Det sagda gäller enligt kommitténs mening särskilt inom arbetslivets område. Det framstår som synnerligen angeläget att de arbetstagarorganisationer som kommer att beröras av koden, involveras i arbetet i ett tidigt skede, och att deras synpunkter beaktas i samband med Datainspektionens prövning av utkastet till kod.

Tillsyns- och normeringsmyndigheter för arbetslivet

Förutom Datainspektionen är Arbetsmiljöverket den myndighet som har tydligast koppling till integritetskydd i arbetslivet.

Arbetsmiljöverket har visserligen inte i någon större omfattning ägnat sig åt frågor som rör personlig integritet i arbetslivet. Frågan berörs dock i verkets föreskrifter. I 10 § tredje stycket Arbetsmiljöverkets föreskrifter (AFS 1998:5) om arbete vid bildskärm sägs att kvantitativ eller kvalitativ kontroll av arbetstagarens arbetsinsats via datasystemet inte får utföras utan dennes vetskap. Vidare anges i Arbetsmiljöverkets rapport *Digital arbetsmiljö*[5] att ”även perspektiv som handlar om integritet, kontroll och övervakning genom exempelvis it-systemens logg och GPS-tracking behandlas alltmer inom en bred definition av begreppet digital arbetsmiljö”.

För övrigt kan noteras att hanteringen av personuppgifter i arbetslivet i Norge regleras bl.a. i den norska arbetsmiljölagen (9 kap. i lov om arbeidsmiljø, arbeidstid og stillingsvern mv.).

Frågor som kan tas upp i uppförandekoder för arbetslivet

Med utgångspunkt i dels de risker som kommittén har bedömt föreligger på arbetslivsområdet, dels de skyldigheter som kommer att åligga arbetsgivarna enligt dataskyddsförordningen, kan uppförandekoder för personlig integritet i arbetslivet beröra bland annat följande frågor (det närmare innehållet kommer att variera beroende på vilken bransch uppförandekoden avser):

- Hur arbetsgivarna ska gå till väga för att uppfylla kravet i artikel 30 i dataskyddsförordningen på register över vilka behandlingar av personuppgifter som görs på arbetsplatsen. Lämpligtvis ges samtidigt en metod eller mall (med exempel) för praktisk inventering och dokumentation av vilka uppgifter om arbetstagarna som hanteras i den utrustning och de system som används på arbetsplatsen, och hur dessa uppgifter används (såväl av arbetsgivaren som av dennes leverantör).
- Hur konsekvensbedömningar avseende dataskydd (artikel 35 i dataskyddsförordningen) ska genomföras före införandet av varje nytt system eller större ändring i befintliga system. Det kan röra sig om att arbetsgivaren tillhandahåller ny utrustning eller ett nytt system för arbetstagarna. Det kan också röra sig om ändrade

[5] Arbetsmiljöverkets rapport 2015:17.

användarvillkor för tjänster som arbetsgivaren redan använder sig av. Det bör även ges en mall eller exempel för hur en konsekvensbedömning kan genomföras i praktiken.

- Hur inbyggt dataskydd och dataskydd som standard (artikel 25 i dataskyddsförordningen) kan genomföras, med angivande av exempel. Exempelvis kan anges att antalet uppgifter ska minimeras och att systemens förhandsinställningar ska vara de mest integritetsvänliga.
- I vilka situationer som behandlingen kan bygga på samtycke från arbetstagarna. Det bör exempelvis anges att tystnad, på förhand ikryssade rutor eller inaktivitet inte ska utgöra ett giltigt samtycke.[6] Vidare kan anges att samtycke inte ska betraktas som frivilligt om arbetatagaren inte har någon genuin eller fri valmöjlighet eller inte utan problem kan vägra eller ta tillbaka sitt samtycke.[7]
- Hur och när uppgifter ska gallras. Uppgifter om inloggningar och enskildas användning av utrustning bör exempelvis kunna gallras eller avidentifieras tämligen omgående i normalfallet, medan det i andra situationer kan vara nödvändigt att spara uppgifterna under längre tid om det är nödvändigt för att genomföra vissa interna kontroller.
- Exempel på informationssäkerhetsåtgärder som arbetsgivarna behöver vidta för att uppfylla kraven i artikel 32 i dataskyddsförordningen (avseende exempelvis behörighet, loggning, säkerhet vid åtkomst över internet osv).
- Vilken information som måste ges till arbetstagarna om hur uppgifter används, med angivande av exempel. Här bör exempelvis anges hur information kan ges med hjälp av standardiserade symboler för att ge en överskådlig, begriplig, lättläst och meningsfull överblick över hur uppgifterna hanteras och av vem.[8]

[6] Se skäl 32 i dataskyddsförordningen.
[7] Se skäl 42 i dataskyddsförordningen.
[8] Se skäl 60 i dataskyddsförordningen.

- När kameraövervakning inomhus kan användas och hur arbetsgivarna bäst kan uppfylla kraven i kameraövervakningslagen på exempelvis dokumentation och information.[9]

Vem ska uppmuntra utarbetandet av uppförandekoder?

Skyldigheten att uppmuntra utarbetandet av uppförandekoder enligt artikel 40 i dataskyddsförordningen gäller inte bara Datainspektionen. Regeringen både kan och bör agera även genom andra myndigheter.

Som framgår i kapitlet om uppförandekoder, anser Integritetskommittén att regeringen så långt som möjligt bör uppdra åt andra myndigheter att i samråd med Datainspektionen stå för merparten av det arbete som en myndighet behöver utföra när det gäller uppförandekoder. Ett skäl till detta är att Datainspektionen inte ska bli överbelastad med uppdrag av detta slag inom en rad olika områden på en gång, samtidigt som myndigheten har ett stort arbete framför sig med att anpassa sin verksamhet till dataskyddsförordningen. Ett annat skäl till detta är att en branschspecifik myndighet i många fall bättre än Datainspektionen känner till vilken slags vägledning (både till form och innehåll) som efterfrågas inom branschen samtidigt som myndigheten inte sällan redan har etablerade kontakter med aktörer och branschföreträdare.

Arbetsmiljöverket har väl etablerade kontakter med olika branscher och har både kunskap om branscherna och även erfarenhet av att samla både arbetsgivarorganisationer och arbetatagarorganisationer för att diskutera frågor om reglering.

Ordet ”uppmuntra” används i dataskyddsförordningen, och ska enligt kommitténs tolkning i detta sammanhang närmast förstås som att initiera och stödja. I arbetet med att initiera och stödja framtagandet av uppförandekoder, kan Arbetsmiljöverket exempelvis bjuda in branschorganisationerna och andra ansvariga myndigheter för ett samtal om förutsättningarna för en uppförandekod på området, där även alternativen till en uppförandekod kan tas upp. Om det inte finns en uppförandekod, måste arbetsgivarna och deras personupp-

[9] Förslag om kameraövervakning kommer att lämnas av Utredningen om kameraövervakning – brottsbekämpning och integritetsskydd (Ju 2015:14) som bl.a. ska ta ställning till om integritetsskyddet i samband med kameraövervakning på arbetsplatser behöver förbättras.

giftsbiträden utan närmare tolkningshjälp enbart tillämpa dataskyddsförordningen eller annan, allmänt hållen ramlagstiftning. Det skulle kunna innebära en ökad risk för administrativa sanktionsavgifter enligt artikel 83 i dataskyddsförordningen.

Det krävs en särskild kompetens för att leda projekt för att ta fram uppförandekoder. Det finns specialister på detta som kan anlitas av myndigheterna för att leda och genomföra sådana projekt, exempelvis inom SIS (Swedish Standards Institute). En möjlighet är att Arbetsmiljöverket utför uppdraget med hjälp av SIS. Det kommer därför inte vara nödvändigt för Arbetsmiljöverket att anställa personer för utförandet av detta uppdrag.

Sammanfattningsvis anser vi att regeringen bör ge Arbetsmiljöverket i uppdrag att i samråd med Datainspektionen vidta åtgärder för att initiera och stödja utarbetandet av uppförandekoder för arbetslivsområdet.

Kommittén vill i sammanhanget betona att uppförandekoderna för arbetslivsområdet inte behöver omfatta samtliga de punkter som nämns ovan – särskilt inte till en början. Det kan vara tillräckligt att specificera tillämpningen när det gäller de företeelser inom arbetslivet som vi bedömer medför de mest allvarliga riskerna för den personliga integriteten: övervakning för att kontrollera arbetstagarnas aktiviteter och beteenden på arbetet. För övervakning av arbetstagarnas aktiviteter och beteenden, är av betydelse bland annat vilka behandlingar och ändamål som arbetsgivaren har laglig grund för, och vilken information som ska ges till de registrerade. Dessa frågor omfattas till en del av Arbetsmiljöverkets ovan nämnda föreskrift[10] på området.

[10] AFS 1998:5.

7 Hälso- och sjukvård och välfärdsteknik inom socialtjänsten

7.1 Riskerna

7.1.1 Hälso- och sjukvård

Integritetskommittén konstaterade i delbetänkandet att allvarliga risker uppstår i samband med informationshantering inom hälso- och sjukvården till följd av:

- bristande ledning och bristande ansvarstagande över informationssystemen och de personuppgifter som hanteras i dessa,
- komplexa miljöer med många olika system för hantering av information, (gamla system),
- brist på gemensamma lösningar, t.ex. gemensam infrastruktur,
- bristande regelefterlevnad,
- bristande kunskaper hos både personal och ledning, samt
- bristande informationssäkerhet.

7.1.2 Användning av välfärdsteknik inom socialtjänsten

Användning av välfärdsteknik kan bland annat handla om att socialtjänsten erbjuder hjälp och stöd åt enskilda med hjälp av olika digitala tjänster i form av trygghetslarm, tele- och videokommunikation, sensorer i hemmet, kognitiva hjälpmedel, ett mobilt arbetssätt och e-tjänster för trygghet, service och delaktighet.

När det gäller användning av välfärdsteknik konstaterade kommittén att risker för den personliga integriteten uppstår till följd av:

- hantering av mycket närgångna och känsliga uppgifter om enskilda med stort hjälpbehov,
- tjänsterna omfattar stora delar av befolkningen,
- oklarheter om hur hantera samtycke vid stöd åt personer med nedsatt beslutsförmåga,
- risk för brister i informationssäkerhet, samt
- bristande ansvarstagande.

7.2 Åtgärd för både hälso- och sjukvården och socialtjänst – uppförandekoder som tillämpningsstöd

Integritetskommitténs förslag: Regeringen bör ge en myndighet i uppdrag att initiera och stödja utarbetandet av uppförandekoder för verksamhet inom hälso- och sjukvård och socialtjänst.

Regeringen bör ge en myndighet i uppdrag att utgöra sekretariat för förvaltningen av de gemensamma uppförandekoderna.

7.2.1 Genomföra visionen om e-hälsa

Det framgår av Vision e-hälsa 2025 att det behövs ett brett nationellt samarbete för att nå visionen. Enligt information på E-hälsomyndighetens webbplats är nyckeln till att förverkliga visionen samverkan mellan alla olika aktörer som arbetar med e-hälsa, allt från kommuner och landsting till idéburna organisationer. E-hälsomyndigheten har enligt sin instruktion ansvaret för att samordna och leda regeringens satsningar.

Inom ramen för visionen om e-hälsa har regeringen och Sveriges kommuner och landsting (SKL) kommit överens om en handlingsplan på e-hälsoområdet för perioden 2017–2019, som bland annat

innehåller en ny nationell samverkans- och samordningsstruktur.[1] Enligt visionen är regelverket ett av insatsområdena. Regeringen och SKL ska enligt handlingsplanen se till att skapa ändamålsenliga regelverk som såväl värnar individens integritet och säkerhet som främjar den digitala utvecklingen, samt underlätta tillämpning och införande av regelverk i berörda verksamheter. Parterna ska därför fastslå en process för att gemensamt identifiera och fånga behov av information gällande befintliga regler eller kommande förändringar av dessa.

Såväl staten som SKL förutsätter alltså ett utvecklat samarbete mellan berörda aktörer inom sektorn.

Den nationella samordnaren för effektivare resursutnyttjande inom hälso- och sjukvården anförde i sitt slutbetänkande[2] att staten behöver ta ansvar för informationshanteringen i hälso- och sjukvården, ur perspektivet att det är en infrastrukturfråga som behöver ges nationellt hållbara och långsiktiga lösningar:

> Det behövs ett tydligt ansvar för nationell informationsstruktur och fackspråk liksom standarder som ska gälla för informationssystemen i både tekniskt och semantiskt hänseende när det gäller utbyte av information m.m. Det behövs krav på och stöd till arbetet med informationshantering. Det behövs också en ändrad lagstiftning som möjliggör informationsutbyte över gränser på ett effektivare sätt än i dag. I slutbetänkandena från Utredningen rätt information i vård och omsorg (SOU 2014:23) liksom från E-hälsokommittén (SOU 2015:32) har förslag lämnats som är väsentliga delar i detta, särskilt vad avser de lagliga och tekniska och organisatoriska förutsättningarna för att utbyta information. Utredningen bedömer att det vore av stor vikt att förslagen nu genomförs för den sammantagna utvecklingen när det gäller informationshantering och verksamhetsstöd i hälso- och sjukvården.

7.2.2 Digitalisering, dataskydd och informationssäkerhet

Informationssäkerhetsarbete beskrivs ofta som ett arbete med att uppnå önskad nivå av riktig, tillgänglig, spårbar samt konfidentiell information i en verksamhet.

Inom hälso- och sjukvården och socialtjänsten måste patientuppgifter finnas tillgängliga där de behövs, och den som använder denna information måste också kunna lita på att den är korrekt. Därför

[1] Handlingsplan för samverkan vid genomförande av vision e-hälsa 2025, 2017–2019, bilaga till regeringsbeslut 2017-01-19 nr III:10, dnr S2017/00378/FS.
[2] *Effektiv vård* (SOU 2016:2), s. 552

måste det finnas skydd som hindrar att information försvinner och att den ändras oavsiktligt eller av någon obehörig person. Det kan innebära en allvarlig risk för enskilda om vårdgivaren eller den som bedriver socialtjänst förlitar sig på felaktig information om honom eller henne. Informationssäkerhet i dessa verksamheter innebär även att obehöriga personer inte ska kunna få tillgång till patientuppgifter.

Av dataskyddsförordningens artikel 32.1 framgår bland annat att den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

7.2.3 Behov av tillämpningsstöd

Patientdatalagen öppnade för nya möjligheter till utbyte av patientinformation genom elektronisk direktåtkomst, men ställer samtidigt höga krav på säkerhet och integritet. För att få dela patientinformation genom elektronisk direktåtkomst krävs att journalsystemen bland annat har inbyggda funktioner för identifiering, behörighetskontroll och loggning. Patienten måste ha möjlighet att, om hon eller han vill, kunna spärra viss eller all information från att delas genom elektronisk direktåtkomst. Innan uppgifter om en patient görs tillgängliga för andra vårdgivare genom sammanhållen journalföring ska patienten också informeras om vad det innebär och att patienten har rätt att motsätta sig att uppgifter lämnas ut till andra vårdgivare. Det har varit en stor utmaning för landstingen att anpassa journalsystemen efter patientdatalagens krav. Trots att lagen infördes den 1 juli 2008 uppfyller landstingen ännu inte dessa krav fullt ut. Enligt den senaste SLIT-rapporten[3] kommer genomförandet av patientdatalagen att bli klart först efter år 2018.

Patientdatalagen är en ramlagstiftning som anger de grundläggande förutsättningarna för informationshantering av uppgifter om patienter inom all hälso- och sjukvård. Riksrevisionens granskning[4] visar att det finns tillämpningssvårigheter och detaljer som inte fullt ut har lösts eller reglerats.

[3] eHälsa i landstingen, maj 2016. En rapport från Landstingens IT-strateger/IT-chefer (SLIT).
[4] Rätt information vid rätt tillfälle inom vård och omsorg – samverkan utan verkan? (RiR 2011:19)

Datainspektionens erfarenhet är att många vårdgivare inte lever upp till bestämmelserna om behörighetsstyrning och åtkomstkontroll enligt patientdatalagen. Många vårdgivare har inte gjort den behovs- och riskanalys som de är skyldiga att göra inför behörighetstilldelning. Det innebär att personal ofta tilldelas alltför omfattande behörigheter och således kan ta del av långt fler patientuppgifter än vad de i praktiken behöver för att ge patienten en god och säker vård. Många vårdgivare har inte heller riktlinjer för vad som utgör obehörig åtkomst, vilket försvårar möjligheterna att genomföra verkningsfulla åtkomstkontroller. Datainspektionen anser att det är av stor vikt att de för integritetsskyddet så viktiga bestämmelserna om behörighetstilldelning och åtkomstkontroll efterlevs på ett godtagbart sätt *innan* förslag genomförs som ger möjlighet till ytterligare spridning av patientuppgifter.[5] Så sent som i april 2017 riktade Datainspektionen skarp kritik mot en region avseende hantering av patientuppgifter. Trots att patientdatalagen trädde i kraft för nästan tio år sedan och trots tidigare kritik från Datainspektionen hade regionen inte vidtagit åtgärder. Datainspektionen förelade regionen att bland annat införa behörighetsbegränsningar i huvudjournalsystemet och att göra en behovs- och riskanalys som ligger till grund för hur man tilldelar behörigheter till användarna.[6]

I delbetänkandet redogjorde vi för uppgifter i tidningen Vårdfokus om att antalet polisanmälningar om dataintrång inom hälso- och sjukvården ökar.[7] Även för att motverka dataintrång är det viktigt att vårdgivarna har tydliga rutiner för hur vårdgivaren förväntar sig att medarbetarna ska använda sig av journalsystemen. Sådana rutiner är viktiga för att hälso- och sjukvårdspersonalen ska kunna känna sig trygga med att de gör rätt och de är nödvändiga för att skydda den enskildes integritet. Vårdgivarna behöver även ha rutiner för att göra polisanmälan i de fall olovligt intrång ändå görs.

[5] Datainspektionens remissvar på SOU 2014:23, dnr 1568-2014
[6] Datainspektionens tillsynsbeslut den 24 april 2017, dnr 1546-2016
[7] SOU 2016:41, s. 255.

Tillämpningsstöd i form av uppförandekoder

En uppförandekod i dataskyddsförordningens mening är en möjlighet för sammanslutningar som företräder personuppgiftsansvariga eller personuppgiftsbiträden att inom en viss bransch eller sektor specificera hur man i praktiken ska tillämpa dataskyddsförordningens bestämmelser.

Ett samarbete mellan personuppgiftsansvariga inom hälso- och sjukvård och socialtjänst om gemensamma uppförandekoder skulle kunna vara ett sätt att lösa tillämpningsproblemen.

Uppförandekoder skulle kunna stärka den ömsesidiga tilliten och samarbetet mellan aktörerna och därmed förutsättningarna att genomföra visionen om e-hälsa 2025, särskilt inom insatsområdet som handlar om regelverket. Också i arbetet med att ta fram riktlinjer och rutiner för t.ex. åtkomst till journalsystemen och för polisanmälan vid dataintrång kan gemensamma uppförandekoder vara ett stöd.

Integritetskommittén bedömer att även inom området välfärdsteknik inom socialtjänsten skulle säkerheten och den ömsesidiga tilliten kunna öka med hjälp av uppförandekoder.

Uppförandekod om gemensam informationsstruktur

Ett sätt att minska onödig spridning av känsliga personuppgifter inom hälso- och sjukvården och socialtjänsten är att strukturera uppgifterna i informationssystemen så att användaren enklare kan ta del av rätt information.

Det pågår nationella arbeten med att ta fram en gemensam informationsstruktur för sektorn. En gemensam struktur är en förutsättning för interoperabilitet, men den gör det också möjligt med smarta lösningar för anpassad tillgång till rätt uppgifter.

Det framgår av den senaste SLIT-rapporten[8] att det finns en bristande interoperabilitet mellan olika system i landstingen. Detta beror enligt rapporten framför allt på bristande standardisering av informatiken i systemen och hur systemen implementerats.

De aktörer som är personuppgiftsansvariga skulle kunna överväga att stärka det gemensamma arbetet genom att ta fram uppförandekoder även för denna aspekt av informationshanteringen. Beroende

[8] eHälsa i landstingen, maj 2016. En rapport från Landstingens IT-strateger/IT-chefer (SLIT).

på syftet med koden och hur den utformas kan en sådan uppförandekod också vara en uppförandekod i dataskyddsförordningens mening.

7.2.4 Normen – en norsk förebild när det gäller uppförandekoder

Det finns förebilder för arbetet med gemensamma uppförandekoder i Norge. Där har man redan i tio år arbetat med en norm för informationssäkerhet för vård- och omsorgssektorn.
Den norska normen för informationssäkerhet är en samling krav och riktlinjer som ska bidra till att skapa en tillfredsställande informationssäkerhet i verksamheterna och i hela sektorn.

Normen[9] har tagits fram av representanter från hälso- och sjukvårds- och socialtjänstsektorn och förvaltas av en särskild styrgrupp där berörda myndigheter, professionsorganisationer, Norsk Helsenett och representanter för regionala huvudmän ingår. Datatilsynet, Direktoratet for forvaltning og IKT (Difi) och Helse- og omsorgsdepartementet deltar som observatörer.

Normen beslutades 2006 för att möta de utmaningar som följde av en ökad elektronisk kommunikation i vård och omsorg. Under 2009 utvidgades Normen till att omfatta inte bara hälso- och sjukvård utan även omsorg och socialtjänst. Direktoratet for e-helse är sekretariat för Normen.

Vård- och omsorgsgivare i Norge är enligt lag skyldiga att använda Helsenettet (motsvarande Sjunet i Sverige) för informationsutbyte. Alla verksamheter som vill ha ett sådant informationsutbyte och vara anslutna till Helsenettet är genom anslutningsavtalet förpliktade att också följa Normen. Den som genom avtalet med Helsenettet har en juridisk förpliktelse att följa Normen ska kunna lita på att andra verksamheter, som också har ett sådant avtal, har tillfredsställande informationssäkerhet för sin behandling av personuppgifter. På så sätt skapas mekanismer så att verksamheterna kan ha ömsesidig tillit till att behandlingen av personuppgifter görs på en god säkerhetsnivå.

Normen är en sammanställning av lagstiftningens krav på informationssäkerhet, men ställer ibland också strängare krav. Det inne-

[9] www.normen.no

bär att Normen ställer krav som specificerar och kompletterar gällande regelverk, men Normen är inte heltäckande. Det finns exempelvis krav i olika lagstiftningar som gäller utöver de krav som finns i Normen.

Normen är indelad i tre delar; en styrande, en genomförande och en kontrollerande del. Den styrande delen beskriver krav på verksamhetens ledning att till exempel ta fram ett ledningssystem för informationssäkerhet och arbeta med riskbedömningar. I den delen som avser genomförande av Normen finns krav som handlar om tillgångsstyrning, autentisering, etablering och drift av informationssystem, avtal och utbildning m.m. Den kontrollerande delen handlar bland annat om säkerhetsrevisioner, avvikelsehantering och åtkomstkontroll.

Normen består förutom av kravdokumentet av vägledningar, mallar, faktaark och utbildningsmaterial. Det finns t.ex. vägledningar om användning av molntjänster, om användning av portallösningar, sms och e-post, om tillgång mellan verksamheter med avtalsexempel vid samarbete om gemensam journal, om informationssäkerhet vid användning av välfärdsteknologi och om sociala medier m.m. Sekretariatet erbjuder även kurser och konferenser.

Lysnarutvalget, en kommitté som hade i uppdrag av Norges regering att utvärdera samhällets digitala sårbarhet, beskriver [10] Normen som en framgångshistoria när det gäller hur hälso- och sjukvårdspersonalen har involverats i arbetet med att ta fram koden. I betänkande anförs också angående Normen att:

> Utvalget observerer at Normen er ønsket velkommen av sektoren, og at den i all hovedsak fungerer bra. Normen gjør at helseforetakene tør å stille krav, og leverandørene blir mer oppmerksomme på temaet ved anskaffelser. Prosessen med å utvikle Normen har hatt en god effekt i seg selv og økt kompetansen i bransjen.

I Norge förebereder man sig nu för att anpassa Normen till dataskyddsförordningen och göra den till en uppförandekod i förordningens mening.

[10] NOU 2015:13 Digital sårbarhet – sikkert samfunn s. 194 och 199.

7.2.5 Uppförandekoder som metod att öka skyddet för den personliga integriteten

Medlemsstaterna och tillsynsmyndigheterna ska enligt artikel 40 i dataskyddsförordningen uppmuntra utarbetandet av uppförandekoder som bidrar till att förordningen genomförs korrekt och med hänsyn till särdragen i olika samhällssektorer. Sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden får utarbeta sådana koder i syfte att specificera tillämpningen av förordningen.

Det är alltså de personuppgiftsansvariga och personuppgiftsbiträden som ska ta fram koderna. Medlemsstaterna och tillsynsmyndigheterna ska uppmuntra arbetet med att ta fram dem.

Av artikel 24.3 dataskyddsförordningen framgår att tillämpningen av godkända uppförandekoder får användas för att visa att den uppgiftsansvarige fullgör sina skyldigheter.

Integritetskommitténs bedömning

Integritetskommittén anser att regeringen bör utse en myndighet som i samråd med Datainspektionen initierar och stödjer arbetet med att ta fram en uppförandekod för hälso- och sjukvård och socialtjänst. Med den norska normen som förebild kan man tänka sig att någon form av representativ styrelse bildas för att fatta de formella besluten om koden och dess innehåll.

Med beaktande av de tillämpningsproblem som vårdgivarna haft avseende patientdatalagen anser kommittén att det är lämpligt att staten tar ett särskilt ansvar för uppförandekoder inom detta område. Genom att knyta ett arbetande sekretariat till utvecklingen och förvaltningen av en sådan uppförandekod kan arbetet med koden bli mer strukturerat och utåtriktat. För att sådana uppförandekoder verkligen ska få genomslag och utgöra stöd i tillämpningen bör uppförandekoderna kompletteras med stödjande insatser och dokument. Sekretariatet för uppförandekoden kan med den norska Normen som förebild anordna utbildningar och konferenser och utarbeta stöddokument, t.ex. vägledningar, faktablad och checklistor. Alla dokument måste förstås godkännas av den partsammansatta styrelsen för koden.

Enligt den nationella samordnaren för effektivare resursutnyttjande inom hälso- och sjukvården[11] behöver verksamhetsstöden samlade insatser från både staten och huvudmännen för att ge den funktionalitet och användbarhet som innebär att de blir ett verkligt stöd i det praktiska arbetet och bidrar till att både spara tid och stärka kvalitet och patientsäkerhet. I utredningen gjordes bedömningen att staten borde avsätta 500 miljoner kronor per år för detta ändamål och att huvudmännen i sin tur borde satsa minst lika mycket.

E-hälsomyndigheten har enligt sin instruktion i uppgift att samordna regeringens satsningar på e-hälsa och ska övergripande följa utvecklingen på e-hälsoområdet.

Integritetskommittén anser att en del av en sådan statlig satsning på verksamhetsstöden kan vara att aktivt stödja huvudmännens arbete med en gemensam uppförandekod genom att bistå med ett sekretariat. Det stämmer väl överens med myndighetens nuvarande uppdrag att E-hälsomyndigheten får fungera som sekretariat för det gemensamma arbetet. Ett annat tänkbart alternativ vore att ge detta uppdrag till Socialstyrelsen.

Mot bakgrund av behovet av gemensamma satsningar för att genomföra visionen om e-hälsa och behovet av tillämpningsstöd när det gäller informationssäkerhet och dataskydd föreslår kommittén att en myndighet, förslagsvis E-hälsomyndigheten, får ett ansvar att initiera och stödja och att vara sekretariat för en eller flera svenska uppförandekoder för informationssäkerhet och dataskydd inom hälso- och sjukvård och socialtjänst.

7.3 Åtgärd – stärka ansvarstagandet

Grundläggande förutsättningar för en ändamålsenlig informationshantering är bland annat att uppgifter finns tillgängliga när de behövs i och för vården av en patient eller i samband med socialtjänstens insatser för en individ. En annan förutsättning är att de uppgifter som dokumenteras förvaras och hanteras på ett sådant sätt att obehöriga inte kan komma åt dem, att uppgifter inte sprids utanför verksamheten, att de informationssystem som används i verksamheten är utformade på ett sådant sätt att integritetsskyddet tillgodoses, att en

[11] *Effektiv vård* (SOU 2016:2), s. 34 och 549 ff.

användares behörighet till uppgifter anpassas och begränsas till de behov som användaren har samt att åtkomsten till uppgifterna loggas och kontrolleras.

7.3.1 Hälso- och sjukvården

Integritetskommitténs förslag: Regeringen bör vidta de utredningsåtgärder som är nödvändiga för att genomföra de förslag till integritetshöjande regler vid hantering av personuppgifter i hälso- och sjukvård (punkt 1–4 nedan), som föreslagits av tidigare utredningar, och föreslå riksdagen att reglerna skyndsamt ska införas i lagstiftningen.

Det är vårdgivaren som har det yttersta ansvaret för informationssäkerheten i verksamheten. Det ansvaret är i dag främst reglerat i patientdatalagen (2008:355) och i Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården. Vårdgivarens övergripande ansvar för kvaliteten i vården regleras i hälso- och sjukvårdslagen (1982:763), patientsäkerhetslagen (2010:659) och i Socialstyrelsens föreskrifter och allmänna råd (SOSFS 2011:9) om ledningssystem för systematiskt kvalitetsarbete.

Utredningen om rätt information i vård och omsorg föreslog i sitt slutbetänkande[12] att vårdgivarens övergripande ansvar för en säker och ändamålsenlig hantering av personuppgifter i verksamheten borde uttryckas tydligare och på ett samlat sätt i den nya Hälso- och sjukvårdsdatalag som utredningen föreslog. Utredningen om rätt information i vård och omsorg föreslog ett helt kapitel med bestämmelser som förtydligade både vårdgivarens och hälso- och sjukvårdspersonalens ansvar för en säker hantering av personuppgifter i verksamheten.

Även E-hälsokommittén[13] lämnade förslag som avsåg att förstärka ledningsansvaret och ansvarstagandet. Kommittén föreslog att patientdatalagen ska kompletteras med ett avsnitt om huvudman-

[12] Utredningens om rätt information i vård och omsorg slutbetänkande *Rätt information på rätt plats i rätt tid* (SOU 2014:23).
[13] E-hälsokommitténs betänkande *Nästa fas i e-hälsoarbetet* (SOU 2015:32).

nens och vårdgivarens ansvar för en ändamålsenlig och säker behandling av personuppgifter.

Den nationella samordnaren för effektivare resursutnyttjande inom hälso- och sjukvården anförde i sitt slutbetänkande[14] att förslagen till en ny hälso- och sjukvårdsdatalag och socialtjänstdatalag som lämnats i betänkandet SOU 2014:23 borde genomföras skyndsamt.

Integritetskommittén anser att regler som syftar till att förtydliga ansvaret för hanteringen av personuppgifter i hälso- och sjukvården och socialtjänsten ligger väl i linje med de förstärkta krav på ansvarstagande som finns i dataskyddsförordningen. I dataskyddsförordningen betonas att de personuppgiftsansvariga ska ansvara för och kunna visa att uppgifter behandlas i enlighet med förordningen (artikel 5.2). Detta kallas i förordningen för ansvarsskyldighet.

Ett argument mot att komplettera patientdatalagen med mer detaljerade bestämmelser skulle kunna vara att följsamheten inte varit så god till de regler som redan finns i patientdatalagen. Integritetskommittén menar dock att en del av tillämpningsproblemen kan bero just på att lagen är en ramlag. Det krävs en aktiv rättstilllämpning för att åstadkomma en bra tillämpning av lagen. Regler som ökar detaljeringsnivån i lagen kan göra det lättare för de verksamheter som ska tillämpa regelverket.

Datainspektionen har avstyrkt[15] förslagen i sin helhet när det gäller betänkandet *Rätt information på rätt plats i rätt tid*[16] och varit kritisk till förslagen i *Nästa fas i e-hälsoarbetet*[17]. Kritiken har dock inte i första hand riktat sig mot de förslag till nya bestämmelser i patientdatalagen, som vi föreslår ska genomföras. Dock var Datainspektionen kritisk till bestämmelsen om att huvudmannen ska ta ansvar för att ställa krav på den personuppgiftshantering som görs i verksamheter som huvudmannen inte bedriver i egen regi. Datainspektionen ansåg att den föreslagna regleringen riskerade att skapa otydlighet genom att det kan uppstå motstridigheter i regelverket. Datainspektionen ansåg att det är viktigt att ansvarsfrågan regleras tydligt och avstyrkte därför förslaget.[18] I övrigt var Datainspektionens kritik främst inriktad på de delar av betänkandenas förslag som

[14] *Effektiv vård* (SOU 2016:2), s. 558.
[15] Datainspektionens remissvar på SOU 2014:23, dnr 1568-2014.
[16] SOU 2014:23.
[17] SOU 2015:32.
[18] Datainspektionens remissvar på SOU 2015:32, dnr 1236-2015.

handlar om ett mer ändamålsenligt informationsutbyte inom och mellan hälso- och sjukvård och socialtjänst.

Kommittén anser att en bestämmelse om att ge huvudmannen ansvar för att ställa krav på och följa upp de verksamheter som bedrivs inom huvudmannens ansvarsområde, inte för med sig att huvudmannen blir personuppgiftsansvarig för den behandling av personuppgifter som andra verksamma vårdgivarna utför. Det uppstår enligt vår mening ingen otydlighet beträffande personuppgiftsansvaret av en sådan regel,

Följande förslag från Utredningen om rätt information i vård och omsorg och E-hälsokommittén (1–4 nedan) bör enligt Integritetskommittén kunna leda till lagstiftning:

1. Säker och ändamålsenlig hantering av personuppgifter.

Kommittén anser att en lag som reglerar personuppgiftshanteringen inom hälso- och sjukvården (patientdatalagen) bör innehålla ett kapitel med bestämmelser om en säker och ändamålsenlig hantering av personuppgifter. I det kapitlet bör bestämmelser om inre sekretess samlas med bestämmelser om ansvaret för att uppgifter finns tillgängliga när det behövs för att arbetet i hälso- och sjukvården ska kunna utföras på ett sätt som tillgodoser enskildas behov av god och säker vård m.m.

Vårdgivaren har, som ovan nämnts, det övergripande ansvaret för informationssäkerheten i verksamheten. Informationssäkerhet handlar bland annat om att de system som innehåller personuppgifter ska vara lätta att använda och i övrigt ändamålsenliga samt att systemen utformas på ett sätt som tillgodoser patienternas behov av integritetsskydd. Tillgång till personuppgifter i hälso- och sjukvården vid rätt tillfälle är en förutsättning för att enskilda patienter ska få en god och säker vård.

Vi anser att bestämmelser som reglerar det övergripande ansvaret för en säker och ändamålsenligt hantering av personuppgifter i hälso- och sjukvården bör samlas i ett särskilt kapitel i den lag som reglerar personuppgiftsansvaret för hälso- och sjukvården. Syftet med att välja ut några särskilt viktiga bestämmelser i detta avseende och lyfta dessa i ett eget kapitel är att betona vårdgivarens och yrkesutövarnas ansvar för att uppfylla lagens syfte. Ett sådant kapitel kan omfatta

dessa nya bestämmelser och relevanta bestämmelser som redan nu finns i patientdatalagen.

2. Huvudmannens ansvar för kravställning

Kommittén anser att det bör införas bestämmelser om att en huvudman, genom att ställa krav på och följa upp de vårdgivare som är verksamma inom huvudmannens ansvarsområde, ska se till att kraven på ändamålsenlig och säker behandling av personuppgifter som ställs i patientdatalagen följs. En huvudman ska se till att de vårdgivare som är verksamma inom huvudmannens ansvarsområde, har sådana informationssystem som kan användas för ändamålsenligt och säkert utbyte av personuppgifter enligt denna lag.

Huvudmannen – ett landsting eller en kommun – har det yttersta ansvaret för att säkerställa att vård erbjuds till i hälso- och sjukvårdslagen angiven personkrets. Vården kan utföras i egen regi, men huvudmannaansvaret innebär ingen skyldighet för huvudmannen att själv bedriva verksamheten, utan driften kan ligga på en fristående vårdgivare.

När hälso- och sjukvård bedrivs genom en vårdenhet som är direkt knuten till huvudmannen är landstinget både huvudman och vårdgivare, men har olika ansvar i de olika rollerna. I förhållande till de privata aktörerna på vårdområdet är kommunen eller landstinget endast huvudman, med visst övergripande ansvar för kommunmedlemmarnas vård men utan bestämmanderätt över vårdgivarens dagliga verksamhet. Varje vårdgivare är också personuppgiftsansvarig för sin hantering av personuppgifter.

Mot bakgrund av det ansvar som huvudmannen har för att landstingets eller kommunens invånare får god vård är det rimligt att huvudmannen ansvarar för en fungerande samverkan mellan vårdgivarna inom det egna ansvarsområdet liksom med andra huvudmän och vårdgivare. En patient ska inte utsättas för sämre kontinuitet i vårdprocessen för att huvudmannen inte bedriver all sjukvård i egen regi. Ifall hälso- och sjukvården inom huvudmannens ansvarsområde bedrivs av flera olika vårdgivare måste dessa kunna utbyta information på ett ändamålsenligt och säkert sätt.

Detta innebär att huvudmannen vid upphandlingen måste ställa vissa grundläggande krav på utformningen av de informationssystem

som utförarna använder, till exempel med avseende på informationsstruktur, termer och begrepp, tekniska krav för användning, utbyte och återanvändning av information, standarder och säkerhetskrav. Huvudmannens ansvar för informationshanteringen inom sitt ansvarsområde bör få en uttrycklig reglering i patientdatalagen.

Ett landsting eller en kommun (huvudmannen) ska ställa krav på och följa upp de vårdgivare som är verksamma inom huvudmannens ansvarsområde, och på så sätt se till att kraven på ändamålsenlig och säker behandling av personuppgifter som ställs i patientdatalagen följs.

Huvudmannens ansvar för att de verksamheter som bedrivs inom ansvarsområdet kan utbyta information på ett lagligt, sätt bör också regleras. Det ska i patientdatalagen uttryckligen ställas krav på att en huvudman ska se till att de informationssystem som används av vårdgivare som är verksamma inom huvudmannens ansvarsområde, kan användas för ändamålsenligt och säkert utbyte av personuppgifter.

3. Dokumenterade personuppgifter ska hanteras och förvaras så att obehöriga inte får tillgång till dem

Kommittén anser att det i patientdatalagen bör finnas bestämmelser om att vårdgivare ska se till att dokumenterade personuppgifter hanteras och förvaras så att obehöriga inte får tillgång till dem. Om internet eller andra jämförliga nät används för att överföra personuppgifter som behandlas enligt patientdatalagen, ska vårdgivaren se till att överföringen görs så att ingen obehörig kan ta del av uppgifterna.

Vårdgivaren, som har det yttersta ansvaret för att verksamheten bedrivs säkert ur alla aspekter, ansvarar också för att se till att dokumenterade personuppgifter hanteras och förvaras så att obehöriga inte kan ta del av dem. Detta gäller redan i dag men är inte tillräckligt uttryckligt reglerat – annat än på föreskriftsnivå. Vi bedömer att detta är en inte helt tillfredsställande lösning med avseende på den omfattande behandling av känsliga personuppgifter som görs inom hälso- och sjukvården. Ansvaret innebär bl.a. att vårdgivaren måste se till att de informationssystem som används i verksamheten är skyddade mot obehörig åtkomst och att det finns bra system för tilldelning av behörighet och för åtkomstkontroll. Bestämmelsen syftar till att

skydda uppgifterna från otilllåten spridning såväl inom som utom verksamheten.

Detta krav på säkerhet vid hantering av personuppgifter över öppna nät regleras idag i Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården.

Den lag som reglerar hanteringen av personuppgifter inom hälso- och sjukvården bör enligt kommittén vara så uttömmande som möjligt ifråga om de integritetsskyddsbestämmelser som det bedöms finnas särskilt behov av för hälso- och sjukvårdens del. Därför anser vi att det bör finns en grundläggande bestämmelse i patientdatalagen eller motsvarande som tydliggör kravet på särskilda säkerhetsåtgärder vid överföring av personuppgifter över internet eller andra jämförliga nät.

4. Krav på informationssystemen

Kommittén anser att det i lagen ska anges att vårdgivare ska se till att de informationssystem som innehåller personuppgifter är lätta att använda, stödjer det kliniska arbetet, underlättar arbetet med kvalitetsutveckling, underlättar samverkan och utbyte av uppgifter samt är utformade på sådant sätt att patienternas integritetsskydd tillgodoses.

Svensk sjukvård har sedan länge en hög datoriseringsgrad. Till exempel har i princip alla landsting it-stöd för all vårddokumentation. Trots detta anser professionernas företrädare att systemen inte alltid ger det stöd i arbetet som behövs för att bedriva en effektiv och säker verksamhet.[19] Ett informationssystem bör stödja yrkesutövaren i arbetssituationen. Systemet bör t ex att underlätta för användaren att göra rätt och motverka att användaren kan göra fel både i systemet och vid utförandet av vårdinsatserna. Ett användarvänligt informationssystem kan öka vård- och omsorgskvaliteten för vårdtagare och personal samt minska kostnaderna för vårdgivaren. Patientdatalagen bör därför kompletteras med en bestämmelse som konkretiserar några av de grundläggande krav som måste ställas på ett informationssystem som innehåller personuppgifter och som ska användas i och för vården av en patient. Vårdgivaren är ytterst

[19] *Störande eller stödjande?* Svensk sjuksköterskeförening, Vårdförbundet, Svenska Läkaresällskapet, Sveriges läkarförbund och Kommunal genomförde projektet ”Om e-hälsosystemens användbarhet 2013”. Arbetet finansierades av Socialdepartementet

ansvarig för att en god och säker vård ges och för hanteringen av personuppgifter i verksamheten. I detta ligger även ett ansvar för att kravställa och upphandla informationssystem som är ändamålsenliga, säkra och kan användas som stöd i arbetet.

Informationssystemen måste vara uppbyggda så att det är möjligt att använda personuppgifter för att fortlöpande och systematiskt utveckla och säkra kvaliteten i verksamheten.

Systemen måste också utformas på ett sådant sätt att den enskildes behov av integritetsskydd tas tillvara vid kvalitetsarbetet. Bland annat måste vårdgivare verka för att inte fler personuppgifter än vad som är nödvändigt med hänsyn till ändamålet används vid kvalitetsarbetet. Informationssystemen kan därför, bland annat, behöva utformas så att användaren inte exponeras för fler personuppgifter än vad som är nödvändigt och att sammanställningar och andra underlag som tas fram vid kvalitetsarbetet inte innehåller personuppgifter som är direkt hänförliga till enskilda individer.

Vårdgivaren ansvarar även för att systemen ska möjliggöra samverkan med andra enheter, verksamheter och vårdgivare. För att lyckas med detta måste vårdgivaren arbeta med informationssystemens struktur och innehåll. Vårdgivaren kan i detta arbete exempelvis få stöd av Socialstyrelsens arbete med en nationell informationsstruktur och ett nationellt fackspråk.

Vidare innebär det övergripande ansvaret för de informationssystem som innehåller personuppgifter, enligt utredningens förslag, ett krav på att utforma systemen på ett sådant sätt att integritetsskyddet tillgodoses. Att direkt i verksamhetssystemen bygga in integritetsskyddande funktioner som gör det lätt för personalen att göra rätt och i stället gör det svårt att göra fel, har stora fördelar.

Kommittén anser i likhet med Utredningen om rätt information i vård och omsorg och E-hälsokommittén att det bör finnas en sådan bestämmelse som uttrycker vårdgivarens ansvar för flera olika aspekter av informationssäkerhet vid hanteringen av personuppgifter i hälso- och sjukvården.

Patientdatalagen behöver också ses över i förhållande till dataskyddsförordningen. Regeringen har därför tillsatt en utredning[20] (Socialdataskyddsutredningen) som ska undersöka vilka konsekven-

[20] Dir 2016:52, Utredningen om dataskyddsförordningen – behandling av personuppgifter och anpassningar av författningar inom Socialdepartementets verksamhetsområde, S 2016:05.

ser dataskyddsförordningen medför i fråga om personuppgiftsbehandling inom Socialdepartementets verksamhetsområde samt analysera vilka anpassningar av författningar som krävs eller bör göras med anledning av den nya EU-regleringen och personuppgiftslagens upphävande. Utredningen ska även undersöka vilka anpassningar av de författningar som hör till Socialdepartementets verksamhetsområde som krävs eller bör göras med anledning av dataskyddsförordningen, och lämna behövliga och lämpliga författningsförslag. Det pågår alltså ett utredningsarbete som bl.a. handlar om patientdatalagen.

Vi bedömer att våra förslag kan beredas tillsammans med de förslag till anpassningar som lämnas av Socialdataskyddsutredningen.

7.3.2 Socialtjänsten

Integritetskommitténs förslag: Regeringen bör, med utgångspunkt i befintliga förslag, låta utreda möjligheten till ny lagstiftning som reglerar hantering av personuppgifter inom socialtjänsten, som kompletterar och specificerar kraven i dataskyddsförordningen.

Integritetskommittén har inte i sin riskanalys analyserat integritetsriskerna som kan föreligga generellt vid hantering av personuppgifter inom socialtjänsten. Vi har i stället begränsat analysen till personuppgiftsbehandling i samband med de tjänster som kan erbjudas enskilda med hjälp av ny teknik, så kallad välfärdsteknik. Det är ett aktuellt område med många pågående satsningar och höga ambitioner. Vid användningen av dessa tjänster uppkommer en rad integritetsfrågor och de förutsätter ofta behandling av personuppgifter.

Statens medicinsk-etiska råd (SMER) har i sin rapport[21] om etiska aspekter på robotar och övervakning i vården av äldre, rekommenderat att en bedömning av de konsekvenser övervakningen kan få för etiska värden ska göras innan övervakningsåtgärder vidtas i vården eller omsorgen av äldre. Rådet betonar särskilt att det är viktigt att balans uppnås mellan nyttan av övervakningen och det intrång i den

[21] *Robotar och övervakning i vården av äldre – etiska aspekter*, rapport av Statens medicinetiska råd Stockjolm 2014.

enskildes integritet som övervakningen innebär. Åtgärden bör vidtas på ett sådant sätt att intrånget blir så begränsat som möjligt.

De bestämmelser som reglerar vilka personuppgifter som får hanteras i socialtjänsten och hur det ska göras är utspridda på en mängd olika författningar. Den nuvarande regleringen av personuppgiftsbehandlingen i socialtjänsten finns i lagen (2001:454) om behandling av personuppgifter inom socialtjänsten, och förordningen (2001:637) om behandling av personuppgifter inom socialtjänsten. Dessutom gäller i vissa delar bestämmelserna i personuppgiftslagen (1998:204). Det finns även regler som rör dokumentation och skyddet av den enskildes integritet på socialtjänstens område i den materiella lagstiftningen såsom socialtjänstlagen (2001:453), och lagen (1993:387) om stöd och service till vissa funktionshindrade. Från och med maj 2018 kommer dataskyddsförordningen ersätta personuppgiftslagen.

Även lagen om behandling av personuppgifter inom socialtjänsten och dess förordning berörs av den pågående utredningen[22] om anpassning till dataskyddsförordningen av regelverket inom Socialdepartementets ansvarsområde.

Utredningen om rätt information i vård och omsorg[23] föreslog en ny socialtjänstdatalag som skulle ersätta lagen om behandling av personuppgifter inom socialtjänsten. Denna lag skulle vara en mer komplett reglering av hur personuppgifter ska hanteras inom socialtjänsten. I sin analys av behovet av ny lagstiftning räknar utredningen upp de brister som föreligger med befintlig lagstiftning[24]:

- Otydligt förhållande mellan lagen om behandling av personuppgifter inom socialtjänsten och personuppgiftslagen.
- Olika regler för olika aktörer på socialtjänstens område.
- Avsaknad av bestämmelser som tydliggör krav på de informationssystem som innehåller personuppgifter.
- Avsaknad av bestämmelser som tydliggör när någon som arbetar i socialtjänsten får ta del av uppgifter.

[22] Utredningen om dataskyddsförordningen – behandling av personuppgifter och anpassningar av författningar inom Socialdepartementets verksamhetsområde, S 2016:05.
[23] SOU 2014:23 s. 631 ff.
[24] SOU 2014:23 s. 591 ff.

– Avsaknad av uttryckliga krav på behörighetsstyrning och åtkomstkontroll.
– Avsaknad av tydlig vägledning för vad som gäller ifråga om utlämnande av personuppgifter på medium för automatiserad behandling och direktåtkomst.
– Bristande harmonisering med motsvarande reglering på hälso- och sjukvårdens område, dvs. patientdatalagen.
– Avsaknad av ett regelverk för ett ändamålsenligt utbyte av uppgifter mellan socialtjänst och hälso- och sjukvård.

Utredningen om rätt information i vård och omsorg anför vidare att en särskild registerlagstiftning i många fall innebär en bättre garanti för utformningen av integritetsskyddet vad gäller särskilt känsliga register. Myndighetsregister med ett stort antal registrerade personer och med ett särskilt integritetskänsligt innehåll bör enligt utredningen vara reglerade i lag. Den behandling av personuppgifter som förekommer inom socialtjänsten är av sådan karaktär och omfattning att de grundläggande principerna för behandlingen ska finnas i en lag. Riksdag och regering har i flera sammanhang uttalat att ett myndighetsregister som behandlar känsliga uppgifter om ett stort antal personer bör regleras i lag.

I sitt remissvar[25] över *Rätt information på rätt plats i rätt tid*[26] anförde Datainspektionen att myndigheten delar uppfattningen att den nuvarande regleringen av personuppgiftsbehandling inom socialtjänsten har vissa brister. Datainspektionen anförde att myndigheten hade uppmärksammat att regleringen är svår att förstå och tillämpa för socialtjänsten. Det är ibland t.o.m. oklart om en viss typ av behandling av personuppgifter ens är tillåten enligt nuvarande lagstiftning. Datainspektionen anförde därför att myndigheten skulle välkomna en ny mer sammanhållen reglering av all den personuppgiftsbehandling som är aktuell inom socialtjänstens område. Enligt Datainspektionens mening fanns det emellertid så stora brister i den föreslagna socialtjänstdatalagen, som inverkar såväl på den faktiska tillämpning av lagen som på det integritetsskydd den enskilde registrerade har rätt till, att föreslaget avstyrktes i sin helhet.

[25] Datainspektionens remissvar på SOU 2014:23, dnr 1568-2014.
[26] SOU 2014:23.

Integritetskommittén delar Datainspektionens och Utredningens om rätt information i vård och omsorg bedömning att det behövs en ny reglering för den personuppgiftsbehandling som förekommer inom socialtjänsten. Personuppgiftsbehandlingen inom socialtjänsten bör i likhet med personuppgiftsbehandlingen i hälso- och sjukvården regleras i en egen lag. En sådan lag bör utformas med beaktande av det lagstiftningsutrymme som dataskyddsförordningen ger. En komplett och tydlig lagstiftning inom detta område ökar förutsättningarna för ett ordnat införande av välfärdsteknik inom socialtjänsten.

Kommittén anser att en sådan lag bör innehålla bl.a. följande.

1. Ett kapitel om en säker och ändamålsenlig hantering av personuppgifter där bestämmelser om inre sekretess samlas med bestämmelser om ansvaret för att uppgifter finns tillgängliga när det behövs för att arbetet i socialtjänsten ska kunna utföras på ett sätt som tillgodoser enskildas behov m.m.
2. Bestämmelser om att den som bedriver verksamhet inom socialtjänsten ska se till att dokumenterade personuppgifter hanteras och förvaras så att inte obehöriga får tillgång till dem. Om internet eller andra jämförliga nät används för att överföra personuppgifter som behandlas enligt socialtjänstdatalagen, ska den som bedriver verksamhet inom socialtjänsten se till att överföringen görs så att ingen obehörig kan ta del av uppgifterna.
3. Bestämmelser om att den som bedriver verksamhet inom socialtjänsten ska se till att de informationssystem som innehåller personuppgifter är lätta att använda, stödjer arbete i socialtjänsten, underlättar arbetet med kvalitetsutveckling, underlättar samverkan och utbyte av uppgifter samt är utformade på sådant sätt att de enskildas integritetsskydd tillgodoses.

Dokumentationen i socialtjänsten är i allmänhet av mer integritetskänslig karaktär än information i många andra sammanhang. Informationen rör inte sällan enskildas privata förhållanden om sådant som exempelvis hälsa och sociala och ekonomiska förhållanden. Av hänsyn till behovet av skydd för den personliga integriteten är det därför nödvändigt att de uppgifter om enskilda som dokumenteras i socialtjänsten hanteras på ett säkert och ändamålsenligt sätt. Det handlar även om att inte äventyra enskildas förtroende för socialtjänstens informationshantering. Samtidigt behöver uppgifter kunna användas

på ett ändamålsenligt sätt som leder till att den enskilde får sina behov tillgodosedda. Dokumenterade personuppgifter behöver därför hanteras på ett sätt som gör att behovet av integritetsskydd kan tillgodoses samtidigt som verksamheten ges förutsättningar att skapa bästa möjliga resultat för enskilda individer.

Grundläggande förutsättningar för en ändamålsenlig informationshantering är bland annat att uppgifter finns tillgängliga när de behövs för att utreda, fatta beslut eller genomföra insatser för enskilda. En annan förutsättning är att de uppgifter som dokumenteras om enskilda förvaras och hanteras på ett sådant sätt att behoven av integritetsskydd tillvaratas. Det handlar exempelvis om att se till att obehöriga inte kan komma åt uppgifter om enskilda, att uppgifter inte sprids utanför verksamheten, att de informationssystem som används i verksamheten är utformade på ett sådant sätt att integritetsskyddet tillgodoses, att en användares behörighet till uppgifter anpassas och begränsas till de behov som användaren har samt att åtkomsten till uppgifterna loggas och kontrolleras m.m.

Integritetskommittén anser att en särskild lag bör reglera personuppgiftshanteringen i socialtjänsten och att en sådan lag bland annat bör innehålla ovan nämnda bestämmelser.

Den utredning[27] som för närvarande undersöker vilka konsekvenser dataskyddsförordningen medför i fråga om personuppgiftsbehandling inom Socialdepartementets verksamhetsområde, har inte till uppgift att föreslå någon ny lag för behandling av personuppgifter inom socialtjänstens område.

7.4 Åtgärd – ställföreträdare för beslutsoförmögna

Integritetskommitténs bedömning: Det behöver införas bestämmelser om legala företrädare för personer med nedsatt beslutsförmåga i vård- och omsorgssituationer. Företrädarna måste ha befogenhet att ta ställning till såväl vård- och omsorgsinsatser, som den personuppgiftshantering som hör ihop med dessa.

[27] Utredningen om dataskyddsförordningen – behandling av personuppgifter och anpassningar av författningar inom Socialdepartementets verksamhetsområde, S 2016:05

Respekten för varje människas integritet och självbestämmande är grundläggande utgångspunkter vid all vård, omsorg och forskning. De lagar som reglerar dessa områden förutsätter många gånger att en vuxen har förmåga att exempelvis själv ta initiativ, lämna samtycke till åtgärder, vara delaktig eller på annat sätt utöva sitt självbestämmande.

Det finns dock personer som inte har förmåga att fullt ut utöva sitt självbestämmande. En persons förutsättningar att ta ställning i frågor, som rör hans eller hennes vård, omsorg eller forskning eller som rör hantering av personuppgifter, kan vara mer eller mindre begränsade. Att inte kunna fatta ett eget beslut i en situation är något som – av vitt skilda orsaker – potentiellt kan drabba alla människor. Personens förmåga att fatta egna beslut i en viss fråga kan vara nedsatt tillfälligt eller under en längre tid och graden av nedsättning kan variera över tid.

Personal inom hälso- och sjukvården och socialtjänsten möter varje dag personer som av en eller annan anledning tillfälligt eller mer varaktigt saknar möjlighet att ge uttryck för sin inställning och vilja att exempelvis få en viss vård- och behandlingsinsats. En sådan person har ofta även nedsatt förmåga ta emot information och lämna samtycke till den informationshantering som vård- och behandlingsinsatserna förutsätter.

Nuvarande regelverk för personuppgiftsbehandling i hälso- och sjukvården och socialtjänsten innehåller inga särskilda bestämmelser för hur personuppgifter avseende personer som saknar förmåga att ta ställning till en viss personuppgiftsbehandling ska hanteras. Det saknas generella och heltäckande regler i svensk rätt gällande i vilka situationer vuxna ska anses sakna förmåga, i rättslig mening, att fatta egna beslut om sin hälso- och sjukvård eller omsorg och vad som då ska gälla.

En konsekvens av bristerna i dagens reglering är bland annat att den som saknar förmåga att ta emot och förstå information samt ta ställning till frågor om informationshantering kan ställas utanför möjligheterna att ta del av de möjligheter som välfärdsteknik erbjuder. Många sådana tjänster är därtill utformade just som stöd för personer som har nedsatt beslutsförmåga och har ökade behov av omsorg och tillsyn.

Denna brist i lagstiftningen har medfört svåra tillämpningsproblem i verksamheter inom vård och omsorg som står inför den kon-

kreta uppgiften att hitta den bästa lösningen för en enskild person i behov av insatser.

Avsaknaden av regler om ställföreträdare för personer med nedsatt beslutsförmåga medför att personer som inte själva kan ta ställning till frågor om hantering av information, riskerar att få insatser på osäkrare villkor och av lägre kvalitet än personer som har förmåga att ta ställning i dessa frågor.

Vår utgångspunkt är att den som saknar förmåga att samtycka till vård eller omsorg och den informationshantering som föranleds av insatsen, har ett alldeles särskilt behov av lagstiftning som ger ökad trygghet och skydd. Behovet av skydd gäller såväl i frågor om patient- och brukarsäkerhet och kvalitet som i frågor om personlig integritet.

Utredningen om stöd och hjälp till beslutsoförmögna i vård, omsorg och forskning har föreslagit en ny lag: lagen om stöd och hjälp till vuxna vid ställningstaganden till hälso- och sjukvård och omsorg[28]. Lagen innehåller bland annat bestämmelser om företrädare för personer som har fyllt 18 år och som inte har förmåga att i olika situationer själva ta ställning i frågor som gäller deras hälso- och sjukvård och omsorg.

Under hösten 2016 lämnade regeringen en lagrådsremiss[29] med förslag till lagstiftning om framtidsfullmakter. En framtidsfullmakt är enligt remissen en fullmakt för en annan person att ha hand om fullmaktsgivarens personliga eller ekonomiska angelägenheter när denne inte längre kan det själv. En framtidsfullmakt ska dock inte kunna omfatta åtgärder inom hälso- och sjukvård eller tandvård. Däremot ska en fullmaktshavare kunna bistå vid ansökan om socialt bistånd och samtycka till personuppgiftsbehandling. Remissen innefattar också förslag om att anhöriga ska få rätt att företräda enskilda som inte längre själva kan ha hand om sina ekonomiska angelägenheter.

[28] *Stöd och hjälp till vuxna vid ställningstaganden till vård, omsorg och forskning* (SOU 2015:80).
[29] Regeringens remiss till lagrådet den 22 september 2016, Framtidsfullmakter – en ny form av ställföreträdarskap för vuxna.

Integritetskommitténs bedömning

Eftersom självbestämmande är en viktig komponent för att den enskilde ska kunna ta till vara sina rättigheter har samhället ett ansvar för att se till att personer med nedsatt beslutsförmåga inte går miste om större värden än absolut nödvändigt, och för att, om möjligt, särskilda åtgärder vidtas för att kompensera för det försämrade skydd som den nedsatta beslutsförmågan för med sig.[30]

För att personer med nedsatt beslutsförmåga ska kunna dra nytta av fördelarna med exempelvis välfärdsteknik med bibehållet integritetsskydd, är det enligt kommittén viktigt att frågan om ställföreträdare får en lösning. Denna fråga blir inte löst av det begränsade förslag till framtidsfullmakter som regeringen lämnade i den ovan nämnda lagrådsremissen.

Kommittén har inhämtat att frågan om ställföreträdare är under beredning i Regeringskansliet. Vi bedömer att det är angeläget att det införs en lagreglerad möjlighet att, i samband med insatser inom hälso- och sjukvården och socialtjänsten, utse någon form av ställföreträdare för vuxna med nedsatt beslutsförmåga.

[30] SOU 2015:80, s. 368.

8 E-förvaltning

8.1 Riskerna

Som framgår av kommitténs delbetänkande, finns det inom e-förvaltningen ett antal risker för den personliga integriteten, relaterade till:

- Den ökade informationsdelningen inom och mellan myndigheter (påtaglig risk).
- När den enskilde förväntas ta ansvar för en hantering som den inte förmår överblicka (kan medföra att risken ökar).
- Offentlig sektors användning av publika molntjänster (allvarlig risk).
- Stora brister i myndigheters kompetens avseende juridik, informationssäkerhet och kravställning (påtaglig risk).
- Myndigheternas användning av tjänster från sociala medier och sökmotorföretagen (viss risk).
- Den ökade spridningen av information från myndigheter till resten av samhället, i kombination med en svårtillämpad och delvis oklar lagstiftning, dvs. PSI-lagstiftningen (påtaglig risk).
- Medborgarprofilering och myndigheters efterforskande verksamhet på nätet (allvarlig risk).[1]
- Bristerna i myndigheternas informationssäkerhet (allvarlig risk).
- Avsaknaden av samordning och styrning (allvarlig risk).

[1] Härmed avses sådan kontrollverksamhet hos myndigheter, som syftar till att i förväg bedöma vilken sannolikhet det finns för att en individ ska begå någon form av felaktighet. Denna typ av kontroller brukar kallas för ”smarta kontroller” eller ”urvalsprofiler”. I delbetänkandet använder vi *medborgarprofilering* som samlingsbegrepp för dessa företeelser.

- Det framkom också att bristerna i regelverket för e-förvaltningen kan medföra försämringar i integritetsskyddet.
- Slutligen kan sägas att en del myndigheter efterlyser tydligare och mer konkret vägledning från Datainspektionen i frågor som rör e-förvaltning.

8.2 Förslag till åtgärder

8.2.1 En myndighet med samlat ansvar för den offentliga förvaltningens digitalisering[2]

Integritetskommitténs förslag: I instruktionen för den myndighet som får det samlade ansvaret för den offentliga förvaltningens digitalisering, bör anges att denna myndighet även ska främja skyddet av den personliga integriteten, och då särskilt stödja lösningar som nyttjar integritetsskyddande arbetssätt och teknik.

Kommittén har i delbetänkandet konstaterat att den bristande styrningen och samordningen i e-förvaltningen innebär risker inte bara för hur snabbt och hur väl digitaliseringen av förvaltningen kan genomföras, utan även bär med sig risker för den personliga integriteten. Vidare har det i kommitténs kontakter med myndigheter framförts att det finns ett behov av tydligare och mer konkret vägledning från Datainspektionen i frågor som rör e-förvaltning och integritetsskydd. Det har likaså i ett antal myndigheters remissvar på delbetänkandet framförts önskemål om tydlig och konkret vägledning från Datainspektionen eller från någon annan myndighet i frågor som rör integritetsskyddet i e-förvaltningen.

Regeringen har gett i uppdrag till Utredningen om effektiv styrning av nationella digitala tjänster att analysera hur digitaliseringen i den offentliga sektorn kan stärkas genom att, inom ramen för den befintliga myndighetsstrukturen, samla ansvaret för dessa frågor till

[2] Med denna myndighet avses det förslag till myndighet med samlat ansvar för digitaliseringen som lämnas i betänkandet *digitalforvaltning.nu* (SOU 2017:23). Integritetskommittén vill betona att alla myndigheter också fortsättningsvis kommer att ha kvar sitt fulla ansvar för hur personuppgifter hanteras av respektive myndighet – även om förslaget införs att ge en myndighet ett särskilt ansvar för digitaliseringen.

en myndighet.[3] Utredningen lämnade i mars 2017 delbetänkandet *digitalforvaltning.nu*.[4] I betänkandet föreslås två alternativ för valet av myndighet där det samlade ansvaret ska placeras. I bägge alternativen föreslås att det i den respektive myndighetens instruktion ska föreskrivas att myndigheten i fråga ska stödja andra myndigheter i utarbetandet av gemensamma uppförandekoder enligt dataskyddsförordningen.

När det gäller hur den ansvariga myndigheten ska arbeta med integritetsskyddsfrågor, anges i delbetänkandet en hög ambitionsnivå:

> Eftersom frågorna om personlig integritet och informationssäkerhet är av avgörande betydelse för att digitaliseringen ska lyckas anser utredningen att de ska utgöra ett särskilt prioriterat område i uppdraget. Det behöver beaktas redan från början i förberedelserna inför att axla det samlade ansvaret för den offentliga sektorns digitalisering. Det ska då knytas sådan kompetens till den myndighet som får uppdraget, som behövs för att beakta integritets- och informationssäkerhetsskydd i ett tidigt skede av olika projekt och uppdrag. I uppdraget ska även ingå att ansvara för samverkan med Datainspektionen, MSB och PTS för att säkerställa att frågorna om skydd av personlig integritet och informationssäkerhet ständigt är närvarande när digitaliseringen genomförs. För att samverkan i frågorna om integritets- och informationssäkerhetsskydd ska prioriteras anser utredningen att de behöver lyftas upp och föras in i respektive myndighets instruktion.

Kommittén välkomnar utredningens förslag och det som sägs om personlig integritet och informationssäkerhet.

För att säkerställa att den höga ambitionsnivå som uttrycks i betänkandet även präglar den ansvariga myndighetens arbete i praktiken, anser vi att ambitionen bör konkretiseras i regeringens styrning av myndigheten även på andra sätt än att myndigheten ska samverka. Vi anser också att integritetsskyddande arbetssätt och teknik bör användas i större omfattning i samhället i allmänhet, och att offentlig sektor spelar en viktig roll i detta. En bilaga till vårt delbetänkande innehöll en inventering av sådan möjlig teknik och arbetssätt.

Det är viktigt att försäkra sig om en genomgående och hög ambitionsnivå i myndighetens arbete när det gäller integritetsskydd och informationssäkerhet. Kommittén anser därför att det i den

[3] N 2016:01.
[4] SOU 2017:23. I det som följer benämns denna myndighet som ”den ansvariga myndigheten”.

ansvariga myndighetens instruktion eller regleringsbrev uttryckligen bör anges att myndigheten även ska främja skyddet av den personliga integriteten, och då särskilt stödja lösningar som nyttjar integritetsskyddande arbetssätt och teknik.[5]

I delbetänkandet konstaterade kommittén att en återkommande iakttagelse är att enskilda i stor utsträckning är omedvetna om och har dåliga kunskaper om hur och varför deras personuppgifter hanteras i it-utrustningar och tjänster i olika sammanhang. En liknande iakttagelse har vi gjort beträffande personuppgiftsansvariga företag och myndigheter. Det finns således ett behov av omfattande och långsiktiga informationsinsatser riktade såväl till allmänheten som till personuppgiftsansvariga myndigheter, företag och övriga organisationer. Vi har därför i kapitlet *Samhällets skyddsmekanismer* lämnat ett förslag om att flera olika myndigheter bör få i uppdrag att inom sitt ansvarsområde utforma och bedriva omfattande folkbildning avseende digitaliseringen och dess inverkan på den personliga integriteten. Vi anser att den myndighet som får det samlade ansvaret, Konsumentverket, Skolverket, Statens medieråd, Datainspektionen samt andra myndigheter och organisationer i civilsamhället borde vara självklara aktörer inom detta område. Dessa måste samarbeta med varandra för att utforma folkbildningsinsatsen på ett så bra och verkningsfullt sätt som möjligt.

Det uppstår ibland på digitaliseringens och integritetsskyddets område motsättningar mellan de myndigheter som driver digitaliseringen och tillsynsmyndigheten. De här motsättningarna har ofta sin grund i respektive myndighets roll och uppdrag, men en bristfällig samverkan mellan myndigheter kan onödigt försvåra utvecklingen av ett välavvägt integritetsskydd och utvecklingen av en effektiv förvaltning. Därför vill vi betona att det är av avgörande betydelse för alla uppdragens genomförande och framgång att den ansvariga myndigheten har ett mycket väl fungerande samarbete med Datainspektionen.

[5] Exempelvis kan detta göras genom att myndigheten i sitt arbete med att stödja och samordna e-förvaltningens utveckling, föreslår eller utreder möjligheterna att, vid samverkan mellan myndigheter eller vid bearbetningar av stora uppgiftssamlingar inom en myndighet, använda sig av integritetsskyddande teknik som intygsbaserad identifiering, randomisering eller säkra flerpartsberäkningar. Dessa exempel är hämtade ur delbetänkandets bilaga 3 *Integritetsskyddande teknik*, där varje teknik beskrivs närmare.

8.2.2 Molntjänster

Integritetskommitténs förslag: Regeringen bör uppdra åt den myndighet som får det samlade ansvaret för den offentliga förvaltningens digitalisering att inrätta ett kompetenscenter för frågor som rör anskaffning och användning av externa it-tjänster.

Regeringen bör också låta utreda hur ett regelverk för tystnadsplikt för leverantörer av molntjänster och andra personuppgiftsbiträden skulle kunna utformas.

Integritetskommitténs bedömning: Kommittén ställer sig bakom förslaget från Statens servicecenter att regeringen i närtid bör initiera ett uppdrag att närmare analysera förutsättningarna för att inrätta en ”statens molntjänst” i enlighet med rapporten från Statens servicecenter.[6]

Kompetenscenter

I rapporten *Molntjänster i staten*, lämnar Pensionsmyndigheten en rad förslag för att förbättra förutsättningarna för den offentliga förvaltningens, särskilt statens, användning av molntjänster. Pensionsmyndigheten skriver bland annat följande.

> För att tillvarata potentialen i molntjänster behöver myndigheter i alla sektorer kunna få stöd och vägledning när de ska köpa externa tjänster. Kunskapen som samlas i ett kompetenscenter behöver vara både bred och djup. Stödet behöver vara både flexibelt och kraftfullt och kräver en organisation för löpande förvaltning. Den aktör som utses som ansvarig bör ha egen erfarenhet av operativ it och erfarenhet av alla perspektiv på externa tjänster – juridik, säkerhet, teknik, organisation m.m. Samarbete bör ske med bl.a. MSB för praktiskt stöd inom området säkerhet. Det bör finnas möjlighet för nyckelpersoner inom it-avdelningar, jurister, säkerhetsexperter, verksamhetsutvecklare m.fl. att söka konsultativt stöd hos kompetenscentret.
>
> Som en del i satsningen på ett kompetenscenter ska den ansvariga aktören tillhandahålla en webportal där man samlar information om internationella standarder, riktlinjer, juridiska och säkerhetsrelaterade vägledningar, avtalsexempel, information om internationella certifieringar m.m. Där bör också finnas aktuell information om EU-projekt och nyheter om andra aktiviteter av intresse på EU-nivå och internatio-

[6] Rapporten *En gemensam statlig molntjänst för myndigheternas it-drift*, Statens servicecenter, 2017.

> nellt. Portalen bör även kunna tillhandahålla blogg eller digitala grupperingar där myndigheter kan utbyta erfarenheter från inköp av molntjänster och erfarenheter av implementeringsprocesser. Till kunskapscentret ska ett nationellt nätverk mellan kontaktpersoner för molntjänstfrågor på olika myndigheter knytas.

Pensionsmyndigheten föreslår därför att det utses en myndighet eller annan aktör som ska tillhandahålla ett kompetenscenter för vägledning och kunskapsutbyte mellan myndigheter i frågor som rör anskaffning och användning av externa it-tjänster. Kompetenscentret ska ge stöd och vägledning till offentliga aktörer i statlig, kommunal och landstingskommunal sektor samt till potentiella leverantörer. Kompetenscentret ska även agera nod för ett nationellt myndighetsnätverk för molntjänster. Pensionsmyndighetens förslag har hittills inte lett till några åtgärder från regeringen.

Kommittén har i delbetänkandet uppmärksammat risker till följd av brister i myndigheternas kompetens när det gäller it-utveckling. Vi ställer oss därför bakom Pensionsmyndighetens förslag. Vi anser att ett sådant kompetenscenter lämpligen bör falla inom ansvarsområdet för den myndighet som får det samlade ansvaret för den offentliga förvaltningens digitalisering.

Kommittén föreslår därför att regeringen uppdrar åt denna myndighet att upprätta och tillhandahålla ett kompetenscenter för frågor som rör anskaffning och användning av externa it-tjänster.

Ett kompetenscenter kan bidra till att den offentliga förvaltningen blir bättre kravställare i upphandlingar, bland annat vad gäller kraven på inbyggd integritet och informationssäkerhet. Bättre och tydligare krav från det allmännas sida, kan även påverka marknaden utanför offentlig sektor.

Tystnadsplikt för leverantörer

I rapporten *Molntjänster i staten*, uppmärksammar Pensionsmyndigheten även avsaknaden av tystnadsplikt för leverantörer. Pensionsmyndigheten skriver bland annat följande.

> Myndigheter behöver kunna anlita privata leverantörer av it-tjänster för att kunna få kostnadseffektiva och moderna it-lösningar som stödjer verksamhetens utveckling. I dagsläget kan offentlighets- och sekretesslagens bestämmelser hindra myndigheter från att lämna ut vissa typer av sekretessbelagda uppgifter till privata it-leverantörer eftersom det saknas

straffrättsligt sanktionerade tystnadsplikter för anställda hos sådana aktörer. Det handlar t.ex. om uppgifter av särskilt integritetskänsligt slag som rör enskilda och som inte bedöms kunna lämnas ut ens om leverantören och dess anställda ingår en avtalsrättslig tystnadspliktsförbindelse.

Om leverantören i stället lyder under en i lag reglerad och straffsanktionerad tystnadsplikt borde det ges större utrymme för myndigheten att lämna ut uppgifterna till leverantören, utan hinder av sekretess, och om det i övrigt är lämpligt, eftersom risken för att uppgifterna obehörigen sprids torde vara relativt låg.

Pensionsmyndigheten föreslår därför att det ska utredas om det är lämpligt och ändamålsenligt att införa en lagreglerad och straffsanktionerad tystnadsplikt för privata leverantörer av it-tjänster, i syfte att underlätta för myndigheter att uppdra åt dessa aktörer att hantera myndighetens sekretessreglerade information.

Kommittén har i sina kontakter med myndigheter fått veta att avsaknaden av tystnadsplikt för leverantörer både ger ett sämre integritetsskydd och försvårar digitaliseringen, genom att det råder tveksamhet om när en myndighet får överlåta åt ett personuppgiftsbiträde att hantera uppgifter. Vi delar därför Pensionsmyndighetens uppfattning i frågan. Vi bedömer att det behövs en utökning av tystnadsplikten och föreslår därför att regeringen låta utreda hur ett regelverk för tystnadsplikt för leverantörer av molntjänster och andra personuppgiftsbiträden skulle kunna utformas. Förslaget bör utformas så att det utgör en balanserad avvägning mellan tystnadsplikten respektive meddelarfriheten.

Statligt moln

I sin rapport *Molntjänster i staten*, föreslår Pensionsmyndigheten även att det bör genomföras en fördjupad analys av förutsättningarna för att inrätta ett eller flera statliga myndighetsmoln och myndighetsgemensamma tjänster i Sverige.

Frågan om ett statligt moln är av betydelse för den personliga integriteten och kan innebära bättre möjligheter att skydda personuppgifter som behandlas av myndigheterna.

Statens servicecenter har som del av ett regeringsuppdrag analyserat förutsättningarna för att skapa en samordnad eller gemensam funktion för delar av statliga myndigheters it-verksamhet. I rapporten *En gemensam statlig molntjänst för myndigheternas it-drift* föreslår

Statens servicecenter att merparten av de statliga myndigheternas it-drift bör samordnas i en statlig molntjänst. Förslaget bör enligt Statens servicecenter rent praktiskt genomföras genom att regeringen i närtid initierar ett uppdrag att närmare analysera förutsättningarna för att inrätta ”statens molntjänst”, som underlag inför ett regeringsbeslut om en sådan tjänst. I uppdraget bör enligt Statens servicecenter ingå att bland annat närmare analysera lämplig verksamhetsform för den statliga molntjänsten och de juridiska förutsättningarna för inrättandet av tjänsten. I rapporten från Statens servicecenter betonas att en statlig molntjänst skulle innebära att it-säkerheten och driftsäkerheten förstärks kraftigt inom staten: ”Med statens molntjänst kommer it-säkerheten för hela statsförvaltningen att bli mycket hög och utan kompromisser”.

Mot bakgrund av de risker och brister som redovisats i delbetänkandet avseende offentlig användning av publika molntjänster, ställer sig Integritetskommittén bakom förslaget att regeringen i närtid bör initiera ett uppdrag att närmare analysera förutsättningarna för att inrätta ”statens molntjänst” i enlighet med rapporten från Statens servicecenter. Kommittén vill i sammanhanget betona vikten av att regeringen i det fortsatta utredningsarbetet även analyserar risker för den personliga integriteten med en statlig molntjänst, exempelvis den omständigheten att många uppgifter från olika myndigheter samlas i en tjänst och således blir tekniskt åtkomliga för personal som arbetar med den statliga molntjänsten.[7]

Även när en statlig molntjänst är i drift, kommer det att finnas ett fortsatt behov av ett kompetenscenter för frågor som rör anskaffning och användning av externa it-tjänster. Det beror dels på att kompetenscentret ska rikta sig även till landsting, kommuner och leverantörer, och dels på att statliga myndigheter kommer att behöva använda sig också av andra externa it-tjänster än dem som kommer att tillhandahållas i den statliga molntjänsten.

[7] Frågeställningen berörs i den nämnda rapporten, exempelvis på s. 58.

8.2.3 Utredning om ”medborgarprofilering”

Integritetskommitténs förslag: Regeringen bör låta utreda hur statliga och kommunala myndigheter arbetar med medborgarprofilering[8], hur myndigheterna bör eller kan arbeta med sådana kontroller, samt föreslå de lagändringar som behövs.

I delbetänkandet konstaterade kommittén att det finns allvarliga risker för den personliga integriteten i sådan kontrollverksamhet hos myndigheter, som syftar till att i förväg bedöma vilken sannolikhet det finns för att en individ ska begå någon form av felaktighet. Denna typ av kontroller brukar ibland kallas för ”smarta kontroller” eller ”urvalsprofiler”. Sådan verksamhet väcker en rad juridiska frågor, som även är grundlagsrelaterade. Frågor väcks både avseende de interna kontrollerna (som görs enbart med uppgifter som finns hos den aktuella myndigheten) och också andra slags kontroller (som görs med användning även av uppgifter som finns hos andra myndigheter, företag och organisationer eller som finns åtkomliga på nätet). Samtidigt framhöll vi i delbetänkandet även att det är synnerligen angeläget, både ur det allmännas och ur medborgarnas perspektiv, att myndigheterna på ett effektivt sätt kan använda sig av egna data och av nätet för att förebygga misstag och oegentligheter.

I delbetänkandet berörs endast två statliga myndigheters arbete med medborgarprofilering. Det finns enligt vår bedömning emellertid anledning att anta att detta slags arbete även förekommer såväl hos andra statliga myndigheter, som i den kommunala sektorn (där det kan tänkas förekomma exempelvis inom ramen för prövningar av rätten till försörjningsstöd eller när kommunala bolag ingår hyresavtal med enskilda personer).

Mot bakgrund av detta, anser kommittén att det finns ett angeläget behov av att kartlägga hur både statliga och kommunala myndigheter arbetar med kontroller och att föreslå de lagändringar som behövs för att ge denna verksamhet en tydlig och legal grund och styrning som beaktar både behovet av kontroller och den enskildes

[8] Härmed avses sådan kontrollverksamhet hos myndigheter, som syftar till att i förväg bedöma vilken sannolikhet det finns för att en individ ska begå någon form av felaktighet. Denna typ av kontroller brukar kallas för ”smarta kontroller” eller ”urvalsprofiler”. I delbetänkandet använder vi *medborgarprofilering* som samlingsbegrepp för dessa företeelser.

personliga integritet och rätten att inte bli diskriminerad. Vi anser därför att regeringen bör låta utreda denna fråga närmare.

I utredningsuppdraget bör ingå att undersöka vilka myndigheter, både statliga och kommunala, som ägnar sig åt medborgarprofilering samt hur dessa kontroller genomförs, exempelvis vilka slags uppgifter som används och vilken betydelse uppgifterna tillmäts. Vidare bör ingå att utreda hur kontroller kan utföras på ett effektivt sätt utan att stå i konflikt med grundläggande bestämmelser om diskrimineringsförbudet i regeringsformen och om integritetsskydd i dataskyddsförordningen och i de registerförfattningar som är aktuella. I uppdraget bör därefter ingå att föreslå en samlad lagstiftning för hur kontroller får genomföras av myndigheter avseende exempelvis vilka uppgifter som får användas och hur uppgifterna får användas. Det bör också utredas vilken information om kontrollerna som ska lämnas till de registrerade, särskilt med avseende på förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt dataskyddsförordningens artiklar 22.1 och 22.4. Det bör utredas även hur det i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade (exempelvis information om de bakomliggande algoritmerna).[9]

8.2.4 Regeringens digitala strategier

Integritetskommitténs förslag: Regeringen bör komplettera sina digitala strategier med en formulering om att Sverige ska bli världsledande på att skydda den personliga integriteten utan att minska takten i digitaliseringen.

I december 2012 presenterade regeringen en strategi för en digitalt samverkande statsförvaltning: *Med medborgaren i centrum*. Strategin förtydligar och preciserar de mål och strategiska ställningstaganden som uttrycks i den förvaltningspolitiska propositionen och i den digitala agendan för Sverige. I strategin sägs bland annat följande.

> … statsförvaltningen spelar en central roll i utvecklingen av Sverige. Den ska vara innovativ, samverkande, rättssäker och effektiv, samt ha en väl utvecklad kvalitet, service och tillgänglighet. Därigenom ska den

[9] Jfr artiklarna 13–15 i dataskyddsförordningen.

> bidra till Sveriges utveckling och ett effektivt EU-arbete. Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter.

Samma ambitionsnivå – att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter – återkommer som det övergripande målet för regeringens nyligen beslutade strategi för hur digitaliseringspolitiken ska bidra till konkurrenskraft, full sysselsättning samt ekonomiskt, socialt och miljömässigt hållbar utveckling.[10]

Mot bakgrund av de brister i integritetsskyddet och informationssäkerheten i den offentliga förvaltningen, som kommittén konstaterade i delbetänkandet, anser vi att regeringens nämnda strategier bör kompletteras med den uttryckliga ambitionen att Sverige ska bli världsledande både på att använda digitaliseringens möjligheter och på att skydda den personliga integriteten, utan att för den skull minska takten i digitaliseringen.

8.2.5 Förhandssamråd och uppförandekoder för e-förvaltningen

Integritetskommitténs bedömning: Integritetskommittén ställer sig bakom förslaget i betänkandet *digitalforvaltning.nu*[11] att den myndighet som får det samlade ansvaret för den offentliga förvaltningens digitalisering, ska stödja andra myndigheter i utarbetandet av gemensamma uppförandekoder enligt dataskyddsförordningen.

Ett allmänt hållet regelverk

Det finns inget särskilt regelverk, utöver personuppgiftslagen, för hur personuppgifter ska hanteras hos myndigheter i allmänhet eller för hur olika myndigheter ska samverka. Från och med den 25 maj 2018 ska dataskyddsförordningen tillämpas, som är allmänt hållen.

Det finns däremot speciella regelverk för vissa områden, som exempelvis patientdatalagen och Socialförsäkringsbalken. Samtidigt finns det hos statliga och kommunala myndigheter ett stort behov av kunskap om hur reglerna ska tillämpas i specifika situationer.

[10] Se *För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi* (dnr N2017/03643/D).
[11] SOU 2017:23.

Förhandssamråd

Många av de frågor om regelverkets tillämpning som uppkommer inom e-förvaltningen, rör specifika projekt. Sådana frågor kommer förmodligen i många fall behöva förhandsgranskas av Datainspektionen enligt det förfarande som i dataskyddsförordningen kallas för förhandssamråd (artikel 36).

Frågor som kan tas upp i uppförandekoder för e-förvaltningen

Det förekommer även att frågor om regelverkets tillämpning inom e-förvaltningen är av mer generell och återkommande natur samt uppstår hos flera myndigheter. I dessa fall behövs det vid tolkning av regelverket en mer allmänt hållen tillämpningshjälp som lämpligen kan ges i form av uppförandekoder (se kapitlet om uppförandekoder) i stället för genom förhandssamråd.

Det är också lämpligt att de vägledningar och riktlinjer som redan finns i dag anpassas till dataskyddsförordningen och till det nationella regelverk som kommer att vara i kraft den 25 maj 2018, och att de görs om till uppförandekoder. Sådana uppförandekoder kan exempelvis handla om följande frågor:

- Elektroniskt informationsutbyte genom direktåtkomst eller genom utlämnande på medium för automatiserad behandling (jfr E-sams[12] vägledning *Elektroniskt informationsutbyte – en vägledning för utlämnande i elektroniskt form*).
- S.k. egna utrymmen hos myndigheter (jfr E-sams vägledning *Eget utrymme hos myndighet*).
- Myndigheters användning av sociala medier (jfr E-sams vägledning *Riktlinjer för myndigheters användning av sociala medier*).

Vidare är det lämpligt att uppförandekoder för e-förvaltningen bemöter dels de risker som kommittén har identifierat inom e-förvaltningen, dels de skyldigheter som kommer att åligga myndig-

[12] E-sam är enligt egen beskrivning ett medlemsdrivet program för samverkan mellan myndigheter och Sveriges Kommuner och Landsting (SKL) om digitaliseringen av det offentliga Sverige. E-sam bildades när E-delegationen upphörde 2015.

heterna enligt dataskyddsförordningen. Det rör sig om exempelvis följande frågor:

- Hur myndigheterna ska gå till väga för att uppfylla kravet på register i artikel 30 dataskyddsförordningen över vilka behandlingar av personuppgifter som görs hos myndigheten. Lämpligtvis ges samtidigt en metod eller mall (med exempel) för praktisk inventering och dokumentation av vilka personuppgifter som hanteras (både av myndigheten och av eventuella leverantörer).
- Hur konsekvensbedömningar avseende dataskydd (artikel 35 i dataskyddsförordningen) ska genomföras före införandet av varje nytt system eller större ändring i befintliga system. Det kan röra sig om att myndigheten börjar använda ett nytt, egenutvecklat system, ska upphandla ett system från en extern leverantör eller införa ändringar i befintliga system eller arbetssätt. Det kan även ges en mall eller exempel för hur en konsekvensbedömning kan genomföras i praktiken.
- Hur inbyggt dataskydd och dataskydd som standard ska införas (artikel 25 i dataskyddsförordningen) med angivande av exempel.
- Exempel på rutiner och riktlinjer för hur skyddade personuppgifter ska hanteras. Exempelvis kan anges att det klart och tydligt måste framgå att personuppgifter är skyddade, till exempel genom flaggning, och att det inte ska råda någon som helst oklarhet om att det är uppgifter som särskilt behöver skyddas.[13]
- Hur och när uppgifter ska gallras, och hur datasskyddsbestämmelserna ska tillämpas i förhållande till arkivregelverket.
- Exempel på informationssäkerhetsåtgärder som myndigheter behöver vidta för att uppfylla kraven i artikel 32 i dataskyddsförordningen (avseende exempelvis behörighetsstyrning, åtkomstkontroll, säkerhet vid åtkomst över internet osv). Exempelvis kan anges att – när utrustning ansluts till internet eller annat öppet nät – bör anslutningen skyddas för att förhindra obehörig trafik. I samma syfte bör åtkomst förhindras från det öppna nätet till annan utrustning eller lokala nät hos den personuppgiftsansvarige.

[13] Se Datainspektionens *Checklista för skolor – Skyddade personuppgifter i skolan* (december 2012).

Om uppgifterna endast får lämnas ut till identifierade användare bör mottagarens identitet säkerställas genom e-legitimation, engångslösenord, aktiva behörighetskort eller motsvarande.

- Vilken information som måste ges till de personer vilkas uppgifter myndigheten hanterar. Här bör exempelvis anges hur information kan ges med hjälp av standardiserade symboler för att ge en överskådlig, begriplig, lättläst och meningsfull överblick över hur uppgifterna hanteras och av vem.[1]
- Andra frågor som kan tas upp i en uppförandekod är kontroller på nätet och i sociala nätverk, och personuppgiftsansvarets placering.

Vem ska uppmuntra utarbetandet av uppförandekoder?

Skyldigheten att uppmuntra utarbetandet av uppförandekoder enligt artikel 40 i dataskyddsförordningen gäller inte bara Datainspektionen. Staten både kan och bör agera genom andra myndigheter. När det gäller den offentliga förvaltningen är det närmast den myndighet som får det samlade ansvaret för den offentliga förvaltningens digitalisering som är aktuell.

Kommittén ställer sig därför bakom förslaget i betänkandet *digitalforvaltning.nu* att den myndighet som får det samlade ansvaret för den offentliga förvaltningens digitalisering, ska stödja andra myndigheter i utarbetandet av gemensamma uppförandekoder enligt dataskyddsförordningen.

Uppmuntrandet kan exempelvis göras genom att myndigheten bjuder in relevanta myndigheter för ett samtal om förutsättningarna för en uppförandekod på ett visst område, där även alternativen till en uppförandekod kan tas upp.

Om det inte finns en uppförandekod, måste myndigheterna utan närmare tolkningshjälp tillämpa dataskyddsförordningen eller annan, allmänt hållen ramlagstiftning. Det skulle kunna innebära en ökad risk för administrativa sanktionsavgifter enligt artikel 83 i dataskyddsförordningen.

[1] Se skäl 60 i dataskyddsförordningen.

9 Konsumentområdet

9.1 Riskerna

Här hanteras flera områden samlat, även om de i delbetänkandet behandlades separat under beteckningarna konsumenter, sociala medier och big data. Dessa områden flyter oftast ihop ur den enskildes perspektiv; exempelvis när sociala medier använder sig av big data i marknadsföringsändamål.

Som framgår av kommitténs delbetänkande, anser vi att det sammantaget finns allvarliga risker för konsumenters personliga integritet, på grund av:

- bristen på information till de enskilda konsumenterna,
- samtyckets urholkning,
- den stora spridningen av uppgifter för nya ändamål, och
- den ökade totala mängden av uppgifter om den enskilde.

Beträffande sociala medier anser kommittén sammantaget att användningen av vissa sociala medier innebär en allvarlig risk för den personliga integriteten, när:

- användandet kan medföra att ett stort antal närgångna uppgifter om den enskilde oavsiktligen exponeras för andra användare,
- det förekommer att sociala medier använder uppgifterna för egna ändamål och sprider dem vidare till andra företag,
- det är svårt för användarna att få klarhet i vilken hantering som kan förekomma, när användarvillkoren väl har godkänts, och

- den enskildes valmöjlighet är begränsad till att antingen godkänna samtliga villkor, eller att avböja och därmed helt ställa sig utanför det sociala mediet.

Kommittén anser att big data för med sig en allvarlig risk för den personliga integriteten, eftersom:

- big data innebär att uppgifter hanteras för nya ändamål som inte är kända vid insamlingen,
- den enskilde förlorar både kännedom om och inflytande över hur uppgifterna hanteras,
- med big data blir det särskilt tydligt att personuppgifter betraktas som en handelsvara med ett högt kommersiellt värde, och
- det finns hög risk för spridning av uppgifterna till parter som inte är kända för den enskilde.

9.2 Förslag till åtgärder

9.2.1 Uppförandekoder

Integritetskommitténs förslag: Regeringen bör ge Konsumentverket i uppdrag att initiera och stödja utarbetandet av uppförandekoder för de branscher där personuppgifter hanteras för huvudsakligen kommersiella ändamål som exempelvis marknadsföring.

Ett allmänt hållet regelverk

Det finns på konsumentområdet inget allmänt regelverk för hur personuppgifter ska hanteras hos företag och andra organisationer. Det är egentligen bara på kreditupplysningsområdet som det finns en speciallagstiftning om integritetsskydd, i form av kreditupplysningslagen. När det gäller aktiviteter på nätet är även vissa bestäm-

melser i lagen (2003:389) om elektronisk kommunikation av betydelse, exempelvis finns här regler om samtycke till kakor (cookies).[1]

Således är det i allt väsentligt personuppgiftslagen som ska tillämpas på området, och från och med den 25 maj 2018 dataskyddsförordningen. Enligt dataskyddsförordningen är möjligheten till nationell lagstiftning som reglerar personuppgiftsbehandling för huvudsakligen kommersiella ändamål mycket begränsad. Såväl personuppgiftslagen som dataskyddsförordningen är allmänt hållna (även om dataskyddsförordningen ställer en del nya, specifika krav på de ansvariga). Det finns därför ett stort behov av kunskap om hur reglerna ska tillämpas i specifika situationer – såväl i dag som efter den 25 maj 2018 då dataskyddsförordningen ska börja tillämpas.

Utöver de regler som tar sikte främst på hur personuppgifter hanteras, finns det flera konsumentskyddande lagar såsom avtalsvillkorslagen och marknadsföringslagen som är av intresse i sammanhanget. Dessa regler kan användas för att stävja otillbörliga affärsmetoder i linje med EU:s konsumenträttsliga regelverk till skydd för konsumenten, som den generellt sett svagare parten i ett avtalsförhållande.

Uppförandekoder

Särskilt när personuppgifter hanteras för huvudsakligen kommersiella ändamål, exempelvis marknadsföring, och när möjligheten till nationell lagstiftning är mycket begränsad, framstår uppförandekoder som ett lämpligt instrument för att specificera hur dataskyddsförordningen ska tillämpas.

Det bör noteras att det på flera områden redan i dag finns fungerande uppförandekoder. Dessa benämns ibland ”branschöverenskommelser” (jfr 15 § personuppgiftsförordningen). I kapitlet om uppförandekoder ger vi exempel på svenska och utländska uppförandekoder. Koder som existerar i dag, bör självfallet beaktas och användas som utgångspunkter i det arbete som föreslås i detta kapitel.

[1] I sammanhanget kan noteras att EU-kommissionen i januari 2017 presenterade ett förslag till ny förordning om respekt för privatlivet och skydd av personuppgifter i elektronisk kommunikation (förordning om integritet och elektronisk kommunikation).

För vilka branscher behövs det uppförandekoder?

När personuppgifter hanteras för huvudsakligen kommersiella ändamål, görs det av en mängd olika aktörer. De frågor som då uppkommer avseende skyddet för den personliga integriteten, varierar beroende på vilken aktör och vilken bransch det rör sig om. Bland de branscher som kommittén har identifierat och där det kommer att behövas närmare vägledning för tillämpningen, finns följande:

- direktmarknadsföring,
- sociala medier,
- mediasajter,
- annonsbörser,
- datamäklare,
- molntjänster,
- e-handel,
- web intelligence, och
- tillverkare och försäljare av uppkopplade saker (Internet of things, IoT), inte minst inom bilindustrin avseende all data som hanteras vid framförandet av moderna bilar.

På grund av de många olika aktörer som finns och de frågor som aktualiseras på området, kommer det med all sannolikhet att behövas flera uppförandekoder om koderna på ett konkret sätt ska kunna ge anvisningar och lösningar på problem som uppstår inom olika sektorer.

Exempelvis finns beträffande uppkopplade saker (IoT) särskilda problem som rör information och samtycke och som bland annat har att göra med att användarna ofta behöver registrera sig i en app för att kunna få full nytta av produkten. Vidare saknar många uppkopplade saker (exempelvis badrumsvågar) egna, lämpliga gränssnitt för hantering av samtycken (som tangentbord eller skärm). Det uppstår också delvis olika frågor beroende på om det rör sig om aktiviteter på nätet såsom e-handel (då en viktig fråga är hur kakor ska hanteras) eller aktiviteter i fysiska butiker (där exempelvis kameraövervakning eller wifi-tracking kan ge upphov till integritetsrelaterade frågor).

Frågor som kan tas upp i uppförandekoder

Med beaktande av såväl de risker som kommittén har bedömt föreligger inom de aktuella områdena, som de skyldigheter som kommer att åligga företagen enligt dataskyddsförordningen, kan uppförandekoder för företag och andra organsationer innehålla närmare anvisningar för tillämpningen av bland annat följande frågor:

- Hur företagen ska gå till väga för att uppfylla kravet i artikel 30 i dataskyddsförordningen på register över vilka behandlingar av personuppgifter som företaget har ansvar för. Lämpligtvis innefattar koden även en metod och mallar (med exempel) för praktisk inventering och dokumentation av vilka uppgifter om enskilda personer som hanteras och hur uppgifterna används (både av företaget och av dess leverantörer).
- Hur företagen, i situationer som typiskt sett uppstår inom respektive områden, ska bedöma sina berättigade intressen i förhållande den registrerades intressen eller grundläggande rättigheter och friheter. Det kan exempelvis anges att en intresseavvägning normalt medför att det är tillåtet att behandla personuppgifter för att upprätta listor över telefonnummer för telefonförsäljning samt att skicka ut direktreklam via branschregister.
- Hur konsekvensbedömningar avseende dataskydd (artikel 35 i dataskyddsförordningen) ska genomföras före införandet av varje nytt system eller arbetssätt samt inför större ändringar i befintliga system eller arbetssätt. Här bör koden tydliggöra vilka nya lösningar eller ändringar som typiskt sett omfattas av kravet på en konsekvensbedömning.
- Hur inbyggt dataskydd och dataskydd som standard (artikel 25 i dataskyddsförordningen) ska införas, med angivande av exempel.
- I vilka situationer pseudonymisering behöver genomföras, med angivande av exempel på olika tillvägagångssätt för pseudonymiseringen.
- Hur den enskildes rätt till dataportabilitet ska tillgodoses och realiseras på ett sätt som underlättar för den enskilde. Det bör då anges standarder för olika områden, exempelvis för webbmejl respektive för appar med funktioner för överföring av text, bild, video och ljud.

- I vilka situationer som behandlingen kan bygga på samtycke från de enskilda personerna. Det bör exempelvis anges att tystnad, på förhand ikryssade rutor eller inaktivitet inte ska utgöra ett giltigt samtycke. Vidare kan anges att samtycke inte ska betraktas som frivilligt om den enskilde inte har någon genuin eller fri valmöjlighet eller inte utan problem kan vägra eller ta tillbaka sitt samtycke.[2] En härmed sammanhängande fråga är när det rör sig om samtycke från minderåriga, då samtycket även eller i stället kan behöva inhämtas från vårdnadshavare. Koden bör även innehålla förslag på lämpliga sätt att inhämta samtycke.
- Exempel på rutiner och riktlinjer för hur skyddade personuppgifter ska hanteras. Exempelvis bör anges att det klart och tydligt måste framgå att personuppgifter är skyddade, till exempel genom flaggning, och att det inte ska råda någon som helst oklarhet om att det är uppgifter som särskilt behöver skyddas.[3]
- Hur och när uppgifter ska gallras. Uppgifter om inloggningar bör exempelvis kunna gallras eller avidentifieras tämligen omgående, medan uppgifter som är relevanta för avtal mellan den enskilde och företaget kan behöva sparas under längre tid.
- Exempel på informationssäkerhetsåtgärder som ett företag behöver vidta för att uppfylla kraven i artikel 32 i dataskyddsförordningen (avseende exempelvis behörighetsstyrning, åtkomstkontroll, säkerhet vid åtkomst över internet osv). Exempelvis kan anges att – när utrustning ansluts till internet eller annat öppet nät – bör anslutningen skyddas för att förhindra obehörig trafik. Om uppgifterna endast får lämnas ut till identifierade användare bör mottagarens identitet säkerställas. Mottagarens identitet kan säkerställas genom e-legitimation, engångslösenord, aktiva behörighetskort eller motsvarande.[4] För uppkopplade produkter (IoT) behöver klargöras vem i leverantörs- eller återförsäljarleden som ansvarar för att tillräckliga informationssäkerhetsåtgärder vidtas.

[2] Se skäl 42 i dataskyddsförordningen.
[3] Jfr Datainspektionens *Checklista för skolor – Skyddade personuppgifter i skolan* (december 2012).
[4] Datainspektionens allmänna råd *Säkerhet för personuppgifter* (november 2008). Exemplen som nämns i detta avsnitt angående tekniska lösningar för att säkerställa mottagarens identitet, ska ses just som exempel på vilken detaljeringsgrad uppförandekoderna bör befinna sig på.

- Vilken information som måste ges till de enskilda, och i förekommande fall till deras vårdnadshavare, om hur uppgifter används, med angivande av exempel. Här bör exempelvis anges hur information kan ges med hjälp av standardiserade symboler för att ge en överskådlig, begriplig, lättläst och meningsfull överblick över hur uppgifterna hanteras och av vem.[5] Informationens innehåll och form bör anges särskilt när det gäller förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt dataskyddsförordningens artiklar 22.1 och 22.4, och hur det i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade (exempelvis information om algoritmer).[6]
- När och hur kameraövervakning eller wifi-tracking inomhus får användas exempelvis inne i butikslokaler.

Branschorganisationer

Det finns ett flertal olika bransch- och intresseorgansationer inom området, som skulle kunna medverka i utarbetandet av uppförandekoder. Bland andra finns SWEDMA (en bransch- och intresseorganisationen för företag och organisationer som arbetar med direkt och datadriven marknadsföring), IAB Sverige (en intresseorganisation för företag inom digital marknadskommunikation med över 200 medlemsföretag), Svensk handel (en arbetsgivarorganisation som driver handelns frågor för parti- och detaljhandeln), Elektronikbranschen (en branschorganisation för leverantörer och handlare inom konsumentelektronik, foto och service), Svensk Elektronik (en branschorganisation för tillverkare, utvecklare och leverantörer inom elektronik), IT & Telekomföretagen (en medlemsorganisation för företag inom it- och telekomsektorn). För konsumenternas intressen, finns Sveriges Konsumenter som är en samarbetsorganisation med 22 medlemsorganisationer.

[5] Se skäl 60 i dataskyddsförordningen.
[6] Jfr artiklarna 13–15 i dataskyddsförordningen.

Vem ska uppmuntra utarbetandet av uppförandekoder?

Skyldigheten att uppmuntra utarbetandet av uppförandekoder enligt artikel 40 i dataskyddsförordningen gäller inte bara Datainspektionen. Staten både kan och bör även agera genom andra myndigheter. När det gäller konsumentområdet är det främst Konsumentverket som är aktuellt. Konsumentverket har också erfarenhet av liknande arbete eftersom verket har ingått överenskommelser med olika branscher i syfte ta fram och precisera villkor. Överenskommelserna betraktas ofta som god sed på marknaden. Ordet ”uppmuntra” används i dataskyddsförordningen, och ska enligt kommitténs tolkning i detta sammanhang närmast förstås som att initiera och stödja.

Konsumentverket arbetar redan i dag med vissa av de frågor som skulle behöva tas upp i uppförandekoder på konsumentområdet. Exempelvis har Konsumentverket erfarenhet av att granska frågor om vilken information konsumenterna ges om datahanteringen, hur samtycke inhämtas och vad som egentligen omfattas av användarvillkor och andra avtal mellan företag och konsumenter. Integritetskommittén noterar att dessa frågor hör till de viktigaste och svåraste för att stärka integritetsskyddet på konsumentområdet. Även i en rapport som Konsumentverket nyligen publicerat, rekommenderar författarna att Konsumentverket ska verka för framtagande av sådana uppförandekoder som förutsätts i dataskyddsförordningen med särskilt fokus på hantering av konsumenters personuppgifter.[7]

Regeringen bör därför ge Konsumentverket i uppdrag att i samråd med Datainspektionen vidta åtgärder för att initiera och stödja utarbetandet av uppförandekoder för de branscher där personuppgifter hanteras för huvudsakligen kommersiella ändamål.

Integritetskommittén bedömer att uppdraget i första hand ska inriktas mot att specificera tillämpningen rörande samtycke respektive intresseavvägning som laglig grund för behandlingen av personuppgifter, samt innehåll och form för den information som ska ges till de registrerade.

I arbetet med att initiera och stödja framtagandet av uppförandekoder, kan Konsumentverket exempelvis bjuda in branschorganisa-

[7] Konsumentverkets rapport 2017:4, *Personuppgifter som betalningsmedel*, författad av Stefan Larsson och Jonas Ledendal.

tionerna och andra ansvariga myndigheter för ett samtal om förutsättningarna för en uppförandekod på området, där även alternativen till en uppförandekod kan tas upp. Om det inte finns en uppförandekod, måste företagen utan närmare tolkningshjälp tillämpa dataskyddsförordningen eller annan, allmänt hållen ramlagstiftning. Det skulle kunna innebära en ökad risk för administrativa sanktionsavgifter enligt artikel 83 i dataskyddsförordningen.

Inom vissa områden kommer det sannolikt vara enklare att få till stånd uppförandekoder, exempelvis för direktmarknadsföring, där det redan finns en branschöverenskommelse och en etablerad branschorganisation. Koder inom andra områden kommer att kräva mer förarbete, som exempelvis när det gäller uppkopplade saker (IoT) där det inte framstår som lika enkelt att identifiera och avgränsa relevanta personuppgiftsansvariga.

Det bör vidare noteras att standarder utgör ett viktigt instrument som stöd för tillverkare och leverantörer av väl utformade produkter och tjänster. Det gäller även integritetsfrågorna. Mot den bakgrunden bör uppförandekoder, när det är möjligt, referera till vedertagna standarder på integritetsområdet. Vidare bör marknadskontrollerande myndigheter följa och delta i standarder som bidrar till regelutvecklandet för den personliga integriteten.

Big data

Big data kännetecknas bland annat av att uppgifter används för nya ändamål, inte sällan okända även för den personuppgiftsansvarige vid tidpunkten för insamlandet. Som vi konstaterade i delbetänkandet innebär big data en rad olika utmaningar för integritetsskyddet. Enligt kommitténs uppfattning innebär utmaningarna dock inte att big data är oförenligt med datskyddsförordningens bestämmelser, varken i teorin eller i praktiken. Förhållandet har på ett träffande sätt utryckts i följande ord av chefen för Information Comissioner's Office:

> It is not a case of big data 'or' data protection, or big data 'versus' data protection. That would be the wrong conversation. Privacy is not an end in itself, it is an enabling right. Embedding privacy and data protection into big data analytics enables not only societal benefits such as dignity,

personality and community, but also organisational benefits like creativity, innovation and trust.[8]

Eftersom big data många gånger innebär att personuppgifter överförs mellan olika medlemsstater i EU eller till länder utanför EU, skulle lösningar på utmaningarna tjäna på att hanteras i ett större sammanhang, än endast på nationell nivå i Sverige.

9.2.2 Tillsyn

Integritetskommitténs förslag: Regeringen bör ge Konsumentverket i uppdrag att, i samråd med Datainspektionen, utöva tillsyn över företeelser, produkter och avtal där integritetsskydd och informationssäkerhet gör sig gällande.

I delbetänkandet konstaterade kommittén att Konsumentverket har uppgett sig ha vissa svårigheter med tillsynen i den digitala miljön. Problemen rör bland annat digital och individanpassad marknadsföring på exempelvis sociala medier, som baseras på en mer eller mindre ingående profilering. Företeelsen har endast i begränsad omfattning varit föremål för Konsumentverkets tillsyn. Likaså har inte användarvillkoren för sociala medier ännu granskats av Konsumentverket. Även i en rapport som Konsumentverket nyligen publicerat, rekommenderar författarna att Konsumentverket ska utveckla metoder för tillsyn som möjliggör insyn i funktion och verkan av individualiserade och datadrivna applikationer för bl.a. marknadsföring.[9]

Det innebär enligt kommitténs uppfattning att det saknas en effektiv tillsyn som har förutsättningar att säkerställa en god efterlevnad av de regler som ska skydda konsumentens personliga integritet. Det gäller både beträffande dataskyddsbestämmelser och konsumentskyddsreglerna (såsom avtalsvillkorslagen eller marknadsföringslagen).

Kommittén anser att regeringen bör verka för en bättre efterlevnad av de konsumentskyddsregler som medverkar till att skydda kon-

[8] *Big data, artificial intelligence, machine learning and data protection*, Information Commissioner's Office (20170301, Version: 2.0).
[9] Konsumentverkets rapport 2017:4, *Personuppgifter som betalningsmedel*, författad av Stefan Larsson och Jonas Ledendal.

sumenters personliga integritet, och för en ökad tillsyn av området. Mot den bakgrunden föreslår vi att regeringen ger Konsumentverket i uppdrag att intensifiera sin tillsyn till skydd för konsumentens personliga integritet. I detta arbete bör Konsumentverket samråda med Datainspektionen.

10 Försäkringsverksamhet

10.1 Bakgrund

I delbetänkandet konstaterade Integritetskommittén att en stor del av försäkringsbolagens verksamhet numera hanteras med hjälp av informationsteknik. Den ökade mängden information som finns tillgänglig om enskilda personer ger försäkringsföretagen möjlighet att få bättre underlag för riskbedömning, skadebedömning och för utredning av oklara försäkringsfall. Företeelsen att med hjälp av sensorer mäta rörelse och aktivitet i bilar och hos personer ger möjlighet att göra riskbedömningen säkrare och mer individanpassad.

10.2 Risker som uppmärksammats i delbetänkandet

I delbetänkandet konstaterade vi alltså att det finns nya integritetsrisker i dag, på grund av att det är möjligt att genom olika former av digitala egenmätningar lämna underlag för beräkning av försäkringspremier, exempelvis för fordonsförsäkring och personförsäkring. Uppgifterna måste hanteras säkert i varje led för att det inte ska uppstå risker för obehörig spridning. Det innebär också ett stort ansvar för bolagen att inte hantera mer känsliga uppgifter än nödvändigt, eftersom tekniken i sig innefattar stora möjligheter till kartläggning av enskilda individers rörelsemönster och livsstil m.m.

Vi konstaterade också att det uppkommer nya risker för att tredjepartsintressenter vill ta del av information om enskilda. Det kan röra sig om uppgifter om hälsa som blir tillgängliga när det exempelvis blir möjligt för patienter att läsa sin patientjournal via internet eller genom att information samlas på olika hälsokonton. Försäkringsföretag kan komma att vilja ta del av uppgifter om kundernas hälsa digitalt genom någon form av app knuten till ett hälsokonto, i stället för att få utskrifter ur patientjournalen. En sådan hantering

förutsätter höga krav på säkerhet vid överföring av uppgifterna och ställer andra krav på den enskilde när det gäller insikter om vad överföringen av uppgifterna kan få för konsekvenser. Detta ställer i sin tur krav på företagen när det gäller ansvar för hanteringen och för information till kunderna. De risker som hör samman med användning av molntjänster uppstår också i samband med att personuppgifter kommer att behandlas av de företag som erbjuder app-tjänsterna.

Den stora mängden uppgifter som finns hos försäkringsföretagen representerar ett betydande ekonomiskt värde och skulle kunna samköras med annan information. Det kan därför finnas en risk för handel med uppgifterna. Försäkringsföretagen omfattas inte av någon lagreglerad tystnadsplikt. Mot denna bakgrund bedömer kommittén i delbetänkandet att det i dag finns påtagliga risker för den personliga integriteten i samband med försäkringsföretagens verksamhet.

Vi anför i delbetänkandet att det finns särskild anledning att följa försäkringsbranschens framtida inriktning. Förutom den tekniska utvecklingen i stort ser vi en utveckling där helt nya informationskällor uppstår, ibland som en följd av potentiella försäkringstagares egna åtgärder. Den här informationen är många gånger av stort intresse för försäkringsbolagen, samtidigt som den kan vara av mycket känslig natur för den enskilde. Vi ser en risk att den här utvecklingen ytterligare rubbar balansen mellan den enskilde försäkringstagaren och dennes försäkringsgivare.

Med tanke på den stora potentiella ökningen av nya informationskällor med känslig information och den tekniska utvecklingen i stort, bedömer kommittén i delbetänkandet att den framtida hanteringen av personuppgifter inom försäkringsverksamheten kan innefatta allvarliga risker för den personliga integriteten.

10.3 Åtgärd – branschen tar fram uppförandekoder

Integritetskommitténs bedömning: Kommittén utgår från att försäkringsföretagen kommer att anpassa sina branschrekommendationer till dataskyddsförordningen. Kommittén utgår också från att företagen i egenskap av personuppgiftsansvariga kommer att ha intresse av att omvandla dessa till uppförandekoder i förordningens mening.

Konsumentverket bör följa försäkringsföretagens arbete med detta och bedöma om det finns behov av stöd från myndigheten.

En uppförandekod i dataskyddsförordningens mening är en möjlighet för sammanslutningar, som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden inom en viss bransch eller sektor, att komma överens om hur man i praktiken ska tillämpa förordningen. Läs mer om uppförandekoder i kapitel 4.

Medlemsstaterna och tillsynsmyndigheten ska enligt förordningen uppmuntra utarbetandet av uppförandekoder. Koderna ska bidra till att förordningen genomförs korrekt. Uppförandekoderna syftar till att underlätta för ansvariga och biträden så att de får stöd i hur de ska göra för att följa förordningen i praktiken.

Det är branschföreträdarna som ska ta fram utkast till en uppförandekod inom sitt område. Utkastet till kod ska sedan granskas och godkännas av tillsynsmyndigheten. Uppförandekoden ska hjälpa till att specificera hur dataskyddsförordningen ska tillämpas.

Svensk Försäkring är försäkringsföretagens branschorganisation. Organisationen utfärdar bland annat gemensamma branschrekommendationer som gäller alla medlemsföretag. Det finns i dag exempelvis följande rekommendationer som har med hantering av personuppgifter att göra:

- Arkivering och information inom personförsäkring
- God sed för försäkring på internet
- Rekommendation om behandling av personuppgifter inom försäkringsföretagens utredningsverksamhet
- Rekommendation om behandling av personuppgifter om hälsa inom försäkringsbranschen
- Rekommendation beträffande försäkringsbolagens hantering av genetisk information
- Rekommendation angående försäkringsbolagens bruk av fullmakter.

Branschen arbetar alltså redan med självreglerande uppförandekoder. Vi bedömer att sådana koder underlättar en korrekt tillämpning av lagstiftningen och därmed också för skyddet av de personuppgifter som hanteras.

Integritetskommitténs bedömning

Nya möjligheter till informationsinhämtning för försäkringsföretagen, genom exempelvis mobila appar, och informationsöverföring, från exempelvis elektroniska journaler och hälsokonton, aktualiserar nya integritetsrisker. Det ställer därför också hårdare krav på företagen vad gäller ansvar, information till kunderna, rutiner och säkerhet.

Dataskyddsförordningen ställer i sin tur tydligare krav på ansvarstagande över hanteringen av personuppgifter. Förordningen erbjuder personuppgiftsansvariga och personuppgiftsbiträden att använda uppförandekoder som ett sätt att arbeta aktivt med tillämpningsfrågor och som ett sätt att kunna visa sitt ansvarstagande. Att ansluta sig till en kod är ett sätt för en personuppgiftsansvarig att visa att den följer förordningen.

Enligt artikel 40 dataskyddsförordningen ska medlemsstaterna och tillsynsmyndigheterna uppmuntra utarbetandet av uppförandekoder som är avsedda att bidra till att förordningen genomförs korrekt. En myndighet kan initiera och stödja utarbetandet av koder genom att bjuda in branschorganisationerna och andra ansvariga myndigheter för samtal om förutsättningarna för uppförandekoder inom området. Förordningen förutsätter dock att det är branschen själv som genom sina företrädare utarbetar uppförandekoderna.

Konsumentverket har enligt sin instruktion bland annat ansvar för att de konsumentskyddande regler som ligger inom myndighetens tillsynsansvar följs och för att stärka konsumenternas ställning på marknaden genom kontakter med privata aktörer och i det arbetet genomföra branschöverenskommelser och insatser på standardiseringsområdet. Konsumentverket har alltså ett uttalat ansvar för att genomföra branschöverenskommelser. Mot den bakgrunden anser kommittén att Konsumentverket bör bevaka om försäkringsföretagen anpassar och utvecklar branschöverenskommelserna till uppförande-

koder i dataskyddsförordningens mening samt överväga behovet att uppmuntra branschen att inleda ett sådant arbete.

Det ingår i Datainspektionens uppdrag enligt dataskyddsförordningen att granska och godkänna de uppförandekoder som försäkringsföretagen tar fram.

Exempel på frågor som kan tas upp i en uppförandekod för försäkringsföretag

Med utgångspunkt i dels de risker som vi har bedömt föreligger inom försäkringsområdet, dels de skyldigheter som kommer att gälla enligt dataskyddsförordningen, kan uppförandekoder inom denna bransch bland annat behandla följande tillämpningsfrågor.

- Hur ett försäkringsföretag ska gå till väga för att uppfylla kravet i dataskyddsförordningens artikel 30 på register över vilka behandlingar av personuppgifter som görs i företaget.
- Konsekvensbedömningar avseende dataskydd (artikel 35 i dataskyddsförordningen) som ska genomföras före införandet av varje nytt system eller större ändring i befintliga system.
- Hur skyddade personuppgifter ska hanteras.
- Hur och när uppgifter ska gallras.
- Vilken information som måste ges till kunderna om hur uppgifter används. Koden kan också beskriva hur information kan ges med hjälp av standardiserade symboler för att ge en överskådlig, begriplig, lättläst och meningsfull överblick över hur uppgifterna hanteras och av vem.[1]

Även mallar eller exempel på hur tillämpningen ska gå till i praktiken, kan ingå i uppförandekoden.

[1] Se skäl 60 i dataskyddsförordningen.

Andra åtgärder än uppförandekoder som dataskyddsförordningen erbjuder

Alla personuppgiftsansvariga bör nu vara i full gång med arbetet att se över sin personuppgiftshantering så att den kan uppfylla de krav som ställs i dataskyddsförordningen. Denna översyn pågår med all sannolikhet också hos försäkringsföretagen. Det innebär en möjlighet för denna bransch ta ett nytt och starkt grepp om dataskyddet. Personuppgiftsansvariga måste enligt dataskyddsförordningen ta ett ledningsansvar för personuppgiftshanteringen och kunna visa att hanteringen är laglig.

Den nya möjligheten till kännbara sanktionsavgifter för de verksamheter som gör sig skyldiga till överträdelser av förordningen är därtill en kraftfull påtryckning.

10.4 Åtgärd – reglerad tystnadsplikt

Integritetskommitténs förslag: Regeringen bör vidta de utredningsåtgärder som är nödvändiga för att genomföra en lagreglerad tystnadsplikt för försäkringsföretagen och deras anställda avseende personuppgifter.

Försäkringsföretagen får i sin verksamhet ta del av ett mycket stort antal uppgifter rörande enskilda personers hälsotillstånd, familjeförhållanden och andra förhållanden av personlig natur. En del uppgifter är till sin karaktär ytterst integritetskänsliga. Modern informationsteknik gör det möjligt för försäkringsföretagen att hantera allt fler uppgifter.

Inom den allmänna hälso- och sjukvården gäller sekretess till skydd för uppgift om enskilds hälsotillstånd och andra personliga förhållanden om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon honom närstående lider men. Motsvarande reglering gäller inom den privat drivna hälso- och sjukvården. Även hos Försäkringskassan gäller sekretess.

När integritetskänsliga uppgifter lämnas ut till ett försäkringsbolag med den enskildes samtycke, har denne ett legitimt intresse av att uppgifterna inte ska komma till obehörigas kännedom.

Till skillnad från vad som gäller inom hälso- och sjukvården och hos myndigheter som hanterar känsliga personuppgifter och till skillnad från vad som gäller inom bankverksamhet avseende kundernas förhållande till banken, så finns det alltså ingen lagreglerad tystnadsplikt som gäller hantering av personuppgifter inom försäkringsverksamheten.

Frågan om lagreglerad tystnadsplikt i försäkringsverksamhet har dock beretts i lagstiftningssammanhang upprepade gånger, men utan att det resulterat i någon lagstiftning. Försäkringsverksamhetsutredningen lämnade redan 1987 ett förslag om en sådan reglering.[2] Därefter har förslag lämnats även av Kommittén om genetisk integritet.[3] Vid remissbehandlingen fick förslaget ett positivt bemötande eller lämnades utan erinran av remissinstanserna. I departementspromemorian *Försäkringsbolags tillgång till patientjournalen*[4] anslöt sig utredningen till kommitténs förslag. Även i departementspromemorian *Sekretess för finansiella företag* lämnades ett förslag om tystnadsplikt.[5] I propositionen *Genetisk integritet m.m.*[6] lämnades ett förslag till riksdagen om en generell tystnadsplikt för anställda i försäkringsbolag angående enskildas förhållanden. Riksdagen avslog dock propositionen i denna del på grund av att det saknades tillräckligt beredningsunderlag för att införa en generell sekretessbestämmelse för hela försäkringsområdet.[7] Regeringen begränsade därför i en senare proposition förslaget om tystnadsplikt till att avse genetisk information som försäkringsbolag får tillgång till.[8] I propositionen uttalade regeringen att en generell bestämmelse om sekretess på försäkringsområdet bör övervägas vid en samlad översyn av sekretesskyddet i finansiell verksamhet. Riksdagen godtog förslaget i denna utformning. En bestämmelse om tystnadsplikt när det gäller genetisk information finns numera i 4 kap. 16 § försäkringsrörelselagen (2010:2043).

[2] Försäkringsverksamhetskommitténs slutbetänkande *Försäkringsväsendet i framtiden* (SOU 1987:58).
[3] Kommitténs om genetisk integritet betänkande *Genetik, integritet och etik* (SOU 2004:20).
[4] Ds 2005:13.
[5] Ds 2011:7.
[6] Regeringens proposition Genetisk integritet m.m., prop. 2005/06:64
[7] Bet. 2005/06:SoU16.
[8] Regeringens proposition Sekretess i försäkringsföretag för uppgift om genetisk undersökning och genetisk information, prop. 2006/07:41.

I lagstiftningsarbetet har argumenten för en lagreglering varit ungefär likalydande. Dessa argument från Försäkringsverksamhetskommittén[9] brukar återges:

> Om lagstiftaren uttryckligen skulle slå fast en allmän sekretess inom det enskilda försäkringsväsendet, skulle detta klargöra för allmänheten och försäkringskunderna att försäkringsbolagen, liksom bankerna, har en tystnadsplikt. Förtroendet för det enskilda försäkringsväsendet skulle härigenom kunna stärkas och diskussioner om själva förekomsten och omfattningen av den s.k. oreglerade försäkringssekretessen skulle kunna upphöra.
>
> En lagfäst sekretess på försäkringsområdet skulle också kunna underlätta arbetet för tjänstemännen i bolagen inte bara genom att förtroendet för försäkringsväsendet skulle stärkas utan också genom att det skulle bli lättare att neka att besvara förfrågningar från obehöriga – enskilda eller myndigheter. Försäkringsbolagens verksamhet skulle också kunna underlättas genom att praxis beträffande försäkringsbolags rätt att utlämna uppgifter kan komma att bli klarare om försäkringssekretessen lagfästs, bl.a. genom ingripanden från försäkringsinspektionen i konkreta fall, genom uttalanden från inspektionens sida och genom en analog tillämpning av banksekretessen.
>
> Om försäkringssekretessen skulle lagfästas, uppnås vidare större likformighet med sekretessförhållandena inom andra områden, där sekretessen redan är lagfäst. /---/
>
> Ett lagfästande av försäkringssekretessen skulle slutligen medföra att sanktionerna för brott mot tystnadsplikten inte kom att enbart avse skadeståndsskyldighet. Försäkringsinspektionen skulle nämligen om försäkringssekretessen var lagfäst, kunna ingripa i konkreta fall mot bolag som inte iakttar tystnadsplikten. Det blir därtill helt klarlagt att sanktioner för brott mot tystnadsplikten kan komma i fråga även om det begåtts av tjänstemän sedan de slutat sin anställning.

Enligt uppgift till kommittén betraktar försäkringsföretagen inkomna uppgifter som strängt konfidentiella och iakttar utan direkt stöd av lag en strikt tystnadsplikt. Det finns också branschrekommendationer om hur personuppgifter ska hanteras.

I departementspromemorian[10] konstateras att det, trots att några allmänna missförhållanden inte torde föreligga, råder stor enighet om att tystnadsplikten inom det enskilda försäkringsväsendet bör författningsregleras. Vidare anförs att det från hälso- och sjukvårdens sida har framhållits vikten av att det införs bestämmelser om tystnadsplikt på försäkringsområdet bland annat för att upprätthålla all-

[9] SOU 1987:58 s. 381
[10] Ds 2005:13 s. 187

mänhetens samt hälso- och sjukvårdspersonalens förtroende för försäkringsbolagen. Även försäkringsbranschen är positiv till detta.

Integritetskommitténs bedömning

Kommittén anser att det är av största vikt att det inte råder någon tvekan om att skyddet för uppgifter om enskildas hälsotillstånd och andra personliga förhållanden kvarstår när de har lämnats till ett försäkringsbolag. Ett klargörande i lag av att försäkringsbolagen har tystnadsplikt skulle enligt vår uppfattning bidra till att såväl hälso- och sjukvårdspersonalens som en bredare allmänhets förtroende för det enskilda försäkringsväsendet stärks.

Kommittén är medveten om att tystnadsplikt för försäkringsföretag och anställda i viss utsträckning också måste kombineras med reglerade undantag, som innebär en skyldighet för företagen att lämna myndigheter vissa begärda uppgifter. Tystnadsplikten kan brytas för viktiga informations- och kontrollbehov för samhället. Exempelvis behöver det finnas undantag från tystnadsplikten i förhållande till Finansinspektionen.

En sekretessbestämmelse behöver också anpassas till vanliga situationer inom försäkringsverksamheten i sig. Vi tänker här exempelvis på reglering av skador inom hemförsäkring och motorfordonsförsäkring. Utlämnande med samtycke från den försäkrade bör förstås också vara möjligt. Försäkringsföretagen måste dessutom ha möjlighet att utreda och anmäla misstänkta försäkringsbedrägerier.

Vi gör samma bedömning angående behovet av en tystnadspliktbestämmelse som omfattar personuppgifter i försäkringsverksamheten som framförts av tidigare utredningar och regeringsförslag. Vi vill särskilt framhålla den betydelse en lagfäst sekretessbestämmelse har för allmänhetens förtroende för försäkringsföretagen. Kommittén anser därför att regeringen med utgångspunkt från befintliga utredningar bör vidta de utredningsåtgärder som är nödvändiga för att genomföra en författningsreglerad tystnadsplikt för försäkringsföretagen och deras anställda.

11 Åtgärder inom några andra områden med allvarliga eller påtagliga risker

11.1 Några andra riskområden som behandlades i kommitténs delbetänkande

I delbetänkandet analyserade Integritetskommittén riskerna för den personliga integriteten även inom områdena bank- och kreditmarknad (kapitel 15), kronofogdemyndighetens verksamhet, kreditupplysning och inkasso (kapitel 16) samt de brottsbekämpande myndigheternas verksamhet (kapitel 18).

11.1.1 Bank- och kreditmarknad

Integritetskommitténs förslag: Regeringen bör låta utreda hur en säker ordning för utfärdande av fysiska legitimationer ska se ut och hur statens ansvar för den ska vara utformad.

Användning av kreditkort och andra digitala transaktioner

I delbetänkandet bedömde kommittén att det finns allvarliga risker för den personliga integriteten förknippade med användning av kreditkort och andra digitala transaktioner. Brottslighet i form av identitetsstölder och bedrägerier är exempel på risker inom området.

Ett sätt att minska riskerna för denna typ av brottslighet är att göra processen för att utfärda och att kontrollera id-handlingar säkrare. Säkra e-legitimationer är också en förutsättning för att utveckla

e-förvaltningen och för att e-handeln ska fungera. E-legitimationernas tillförlitlighet är därför ett viktigt samhällsintresse.

Det finns ett flertal aktörer som utfärdar fysiska legitimationer. Myndigheter som Transportstyrelsen, Skatteverket och Polisen utfärdar enligt Svensk bankförening 95 procent av de fysiska legitimationer som bankerna accepterar.

Bankföreningen har i sitt remissvar[1] över kommitténs delbetänkande anfört att e-legitimationer till skillnad mot fysiska legitimationer möjliggör kontroller i realtid av legitimationens giltighet. Detta menar Bankföreningen är en klar säkerhetsfördel med e-legitimationer jämfört med fysiska legitimationer. Utmaningar för bankerna med att utfärda e-legitimationer (BankID) består i att säkra steget från en fysisk legitimation till en e-legitimation. Utgångspunkten för en e-legitimation är alltid att det finns en fysisk legitimation. Det är svårt att avgöra om den fysiska legitimationen som presenteras är äkta eller falsk, eftersom förfalskningar ofta är skickligt gjorda och kontrollmöjligheterna av fysiska legitimationer är begränsade. För att skapa en tillförlitlig process för identifiering och utfärdande av legitimationer i Sverige anser Bankföreningen att det bör införas en gemensam nationell utfärdandeprocess. Bankföreningen anser att det är en uppgift för staten att fastställa en persons identitet och utfärda en fysisk legitimation baserad på sådan information.

Även E-legitimationsnämnden har identifierat detta problem. I en rapport[2] från 2016 rekommenderar nämnden att regeringen ska ge en myndighet i uppdrag att tillhandahålla en sådan grundidentifiering av fysiska personer som i vissa fall behöver genomföras med hjälp av personliga besök eller motsvarande i samband med nyutfärdande av svenska e-legitimationer. En sådan myndighet behöver ha mycket god kompetens att kontrollera personers identitet och ha lokal representation i varje län. Nämnden motiverar denna rekommendation med att det är kostsamt och svårt för e-legitimationsutfärdare att sköta den initiala grundidentifiering av användaren som i vissa fall behöver göras genom personligt besök i samband med nyanskaffning av en e-legitimation. Detta riskerar att göra det dyrt för myndigheter eller för medborgare. Samtidigt är detta en central komponent för att

[1] Remissyttrande från Svenska bankföreningen den 11 november 2016, 2016/08/006.
[2] Fortsatt försörjning av tjänster för e–legitimering och e-underskrift, den 25 oktober 2016, dnr 131 645711–15/9513.

bygga tillit för e-legitimationerna. Nämnden ser därför att staten behöver utöka sitt ansvar i samband med identifiering av personer som ansöker om svenska id-handlingar. Syftet är dels att underlätta vid nyutgivning av innovativa och säkra e-legitimationer, dels att motverka id-kapningar och annat missbruk. E-legitimationsnämnden anser vidare att det vid nyutfärdande av fullvärdiga fysiska legitimationer är nödvändigt att lagra biometri i de fysiska id-handlingarna så att det kan användas vid id-kortskontroller. För att få full säkerhet krävs att individens biometri jämförs med tidigare utfärdade handlingar för samma identitet. Endast fullvärdiga svenska fysiska id-handlingar som innehåller biometri bör ligga till grund för e-legitimationer på den högsta svenska tillitsnivån.

Integritetskommitténs bedömning

Kommittén delar Bankföreningens och E-legitimationsnämndens bedömningar. Det är en viktig integritetsfråga att det finns ett gott skydd för enskildas identiteter. Staten bör därför ta ett ansvar för att få till stånd en säker ordning för utfärdande och kontroll av fysiska legitimationer. Vi anser att regeringen bör låta utreda frågan om hur en säker nationell process av utfärdande av fysiska legitimationer ska se ut och hur staten kan ta ansvar för den. Utredningen bör omfatta frågan om detta ska vara en myndighetsuppgift.

Frågan om e-legitimationer och hur en infrastruktur ska se ut utreddes också av Utredningen om bildande av en e-legitimationsnämnd.[3] E-legitimationsnämnden har så sent som i oktober 2016[4] lämnat förslag på lösningar vad gäller bland annat frågan om fysisk identifiering. De utredningsinsatser som kan bli aktuella för Regeringskansliet i den här frågan bör därför kunna bli mindre omfattande.

[3] Utredningens om bildande av en e-legitimationsnämnd betänkande *E-legitimationsnämnden och Svensk e-legitimation* (SOU 2010:104).
[4] Fortsatt försörjning av tjänster för e–legitimering och e-underskrift, den 25 oktober 2016, dnr 131 645711–15/9513.

11.1.2 Kreditupplysningsföretagens verksamhet

Integritetskommittén behandlade riskerna vid kreditupplysningsföretagens verksamhet i delbetänkandets[5] kapitel 16 om Kronofogdemyndighetens verksamhet, kreditupplysning och inkasso.

Integritetskommitténs bedömning: Det är angeläget att regeringen lämnar förslag på reglering som ger integritetsskydd vid utlämnande av kreditupplysning, oavsett hur kreditupplysningen lämnas ut. Detta kan göras med utgångspunkt i förslag som redan föreligger.

Integritetskommitténs förslag: Regeringen bör låta utreda möjligheten till en författningsreglerad rättighet för fysiska personer att vända sig till den som ger ut en kreditupplysningspublikation för att få uppgifter om sig själv strukna innan uppgifterna publiceras.

Lagstiftningsarbete som pågår

Flera av de integritetsskyddande reglerna i kreditupplysningslagen (1973:1173) gäller inte för utlämnande av kredituppgifter med hjälp av tekniska upptagningar. Förutsättningen för undantagen är att informationen lämnas ut på en teknisk upptagning som omfattas av bestämmelserna om *utgivna* tekniska upptagningar i 1 kap. 10 § yttrandefrihetsgrundlagen. Ett utlämnande på ett usb-minne kan under vissa förutsättningar räknas som en sådan utgiven teknisk upptagning. De skyddande bestämmelserna som då inte ska gälla är exempelvis bestämmelserna om legitimt behov, lämnande av kreditupplysningskopia och skyldigheten att sända en rättelse eller komplettering till var och en som har mottagit en upplysning med en oriktig eller missvisande uppgift eller en uppgift som har behandlats i strid mot lagen.

Mot bakgrund av att skyddsreglerna inte fungerar på det sätt som lagstiftaren egentligen avsett, bedömer kommittén i delbetänkandet att det föreligger allvarliga risker för den personliga integriteten i

5 SOU 2016:41, s. 437 och 446 ff.

kreditupplysningsföretagens verksamhet. Vi noterar dock att denna fråga har utretts[6] och för närvarande bereds i Regeringskansliet. I en promemoria från 2013 föreslås att samtliga former av utlämnanden av kreditupplysningar på sätt som avses i yttrandefrihetsgrundlagen bör omfattas av kreditupplysningslagens skyddsregler med krav på legitimt behov, kreditupplysningskopia och rättelse.

Kommittén bedömer att det är angeläget att regeringens beredning leder till en reglering som ger ett gott integritetsskydd oavsett hur kreditupplysningen lämnas ut. Det är också viktigt att en sådan reglering fortsatt bidrar till en effektivt fungerande kreditupplysningsverksamhet.

Ytterligare lagstiftningsåtgärder – den enskildes rätt att bli struken

Skatteverket lämnar ut offentliga uppgifter från beskattningsdatabasen i elektronisk form till kreditupplysningsföretag. Uppgifter i beskattningsdatabasen får lämnas ut på medium för automatiserad behandling till den som har tillstånd att bedriva kreditupplysningsverksamhet eller som bedriver kreditupplysningsverksamhet som är undantagen från tillståndsplikt.

Skatteverket har i ett yttrande över departementspromemorian *Ett starkare stöd för den enskildes integritet vid kreditupplysning*[7] och i ett yttrande över departementspromemorian *Ett teknikoberoende skydd för den enskildes integritet vid kreditupplysning*[8] föreslagit ett utökat integritetsskydd vid kreditupplysningar i form av en rätt för den enskilde att begära att uppgifter som lämnats ut inte publiceras.

Skatteverket vidhåller i sitt remissyttrande[9] över kommitténs delbetänkande detta förslag om strykningsrätt när det gäller offentliggörande på ett sådant sätt som avses i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Skatteverkets förslag innebär en författningsreglerad rättighet för fysiska personer att vända sig till den som ger ut en kreditupplysningspublikation för att få uppgifter om sig själv strukna innan upp-

[6] Ds 2008:34, Ds 2013:27.
[7] Ds 2008:34.
[8] Ds 2013:27.
[9] Skatteverkets dnr 131 321192–16/112.

gifterna publiceras. En sådan rätt skulle ge den enskilde en möjlighet att hindra att ekonomiska uppgifter om denne sprids fritt i samhället.

Kommittén anser att Skatteverkets förslag skulle öka den enskildes inflytande över spridningen av sina personuppgifter. Vi anser därför att regeringen bör låta utreda detta och ta fram ett förslag inom ramen för det som är förenligt med tryckfrihetsförordningen och yttrandefrihetsgrundlagen.

11.1.3 De brottsbekämpande myndigheternas verksamhet

Integritetskommitténs förslag: Regeringen bör låta utreda en lagreglering av sådana integritetskänsliga spaningsmetoder som i dag inte är reglerade eller har svag reglering.

Polismetoder med svag eller obefintlig reglering

När det gäller de brottsbekämpande myndigheternas verksamhet gjorde kommittén i delbetänkandet bland annat bedömningen att det finns påtagliga risker för den personliga integriteten när det gäller vissa integritetskänsliga spaningsmetoder. Det gäller exempelvis användning av dolda kroppsmikrofoner, handmanövrerade kameror, kopiering av mobiltelefoner och datorer och pejling. Även användningen av falska basstationer och installation av spionprogram är exempel på sådana spaningsmetoder.

Tidigare har även Integritetsskyddskommittén[10] tagit upp dessa risker. Integritetsskyddskommittén konstaterade att polisen för att kunna fullgöra sina uppgifter är beroende av spaningsmetoder som innebär någon form av avlyssning eller övervakning och som många gånger görs i hemlighet. Vissa metoder förutsätter att tekniska hjälpmedel används, såsom handmanövrerad kamera, dold kroppsmikrofon, inspelningsapparatur och pejlingsutrustning. Även om lagenligheten av en del av dessa metoder genom åren har ifrågasatts från olika håll, menade Integritetsskyddskommittén att bedömningen inte kan göras att polisen bör avstå från att i nuvarande omfattning

[10] Integritetsskyddskommitténs delbetänkande *Skyddet för den personliga integriteten* (SOU 2007:22), del 1, s. 472.

använda de aktuella metoderna på grund av att de alltför mycket inkräktar på den personliga integriteten. Däremot var det enligt Integritetsskyddskommittén önskvärt att integritetskänsliga spaningsmetoder blir föremål för reglering.

Polismetodutredningen[11] föreslog år 2010 en sådan reglering. Utredningen föreslog bland annat att spaningsmetoder som behöver lagregleras ska tas in i en ny lag om särskilda inhämtningsåtgärder i de brottsbekämpande myndigheternas verksamhet (inhämtningslagen). Lagen skulle bland annat innehålla bestämmelser om när polisen får använda dolda kroppsmikrofoner, handmanövrerade kameror och s.k. pejling. I den delen syftade förslaget till att stärka den personliga integriteten och innebar bland annat att upptagning med sådan utrustning endast skulle få förekomma dels i förundersökning om åtgärden kan antas vara av särskild betydelse för utredning av brott för vilket är föreskrivet fängelse i ett år eller däröver, dels i underrättelseverksamhet om det finns särskild anledning att anta att åtgärden kan bidra till att förebygga, förhindra eller upptäcka brott av angivet slag. Utredningens förslag har i denna del inte lett till någon lagstiftning.

Utredningen om 2016 års dataskyddsdirektiv[12] har i uppdrag att utreda hur EU:s direktiv om skydd av personuppgifter vid brottsbekämpning, brottmålshantering och straffverkställighet ska genomföras i svensk rätt. Utredningen har i delbetänkandet *Brottsdatalag*[13] föreslagit en ramlag med generella regler för personuppgiftsbehandling inom direktivets område.

Integritetskommitténs bedömning

Kommittén delar Integritetsskyddskommitténs bedömning att det oreglerade tillstånd som råder, medför betydande risker för att det lokalt eller på individnivå beslutas om spaningsmetoder som inte tillräckligt beaktar integritetsskyddsintresset. Det är först genom en reglering som det blir möjligt att generellt dra rågången mellan tillåtna och icke tillåtna metoder samt att ta ställning till andra frågor av betydelse för integritetsskyddet, som till exempel vem som ska ha

[11] Polismetodutredningens betänkande, *Särskilda spaningsmetoder* (SOU 2010:103).
[12] Ju 2016:06.
[13] Utredningens om 2016 års dataskyddsdirektiv delbetänkande *Brottsdatalag* (SOU 2017:29).

behörighet att besluta om teknisk spaning och vilka kompensatoriska skyddsåtgärder som behövs.

Vi anser därför att regeringen bör låta utreda en lagreglering av integritetskänsliga spaningsmetoder med svag eller obefintlig reglering.

12 Informationssäkerhet

12.1 Riskerna

I delbetänkandet konstaterade Integritetskommittén att det finns starka indikationer på väsentliga brister i informationssäkerheten hos offentliga organisationer, t.ex. i organisationer med mycket omfattande personuppgiftsbehandlingar som i kommunerna. Beträffande e-förvaltningen bedömde kommittén att dessa brister måste sägas medföra en allvarlig risk för den personliga integriteten.

Vi konstaterade också att bristerna i informationssäkerheten medför ett sämre skydd för den personliga integriteten. Med tanke på att ett antal av de skyddsåtgärder som rekommenderas av bland annat OECD och Enisa, som exempelvis anonymisering, pseudonymisering och kryptering, är svåra att införa inom vissa samhällssektorer, finns det ett behov av samordning på nationell nivå, till exempel när det gäller standarder och normer. Det finns även ett behov av att i högre grad integrera arbetet med att skydda den personliga integriteten med det traditionella informationssäkerhetsarbetet.

12.2 Åtgärder

12.2.1 Pågående arbete

Det pågår en rad olika utredningar och satsningar i Sverige och på EU-nivå som syftar till att förbättra informationssäkerheten i samhället. Bland dessa kan följande särskilt noteras.

I juli 2016 antog Europaparlamentet och rådet det s.k. NIS-direktivet.[1] Direktivet fastställer åtgärder för att uppnå en hög

[1] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

gemensam nivå på säkerhet i nätverk och informationssystem inom unionen, i syfte att förbättra den inre marknadens funktion. Direktivet innebär bland annat skyldigheter för vissa leverantörer av samhällsviktiga tjänster och vissa leverantörer av digitala tjänster att vidta säkerhetsåtgärder för att hantera risker samt förebygga och hantera incidenter i nätverk och informationssystem som de är beroende av för att tillhandahålla tjänsterna. Leverantörerna ska också rapportera incidenter som har en betydande respektive avsevärd inverkan på kontinuiteten i tjänsten. I maj 2017 lämnade Utredningen om genomförande av NIS-direktivet betänkandet *Informationssäkerhet för samhällsviktiga och digitala tjänster*[2] som innehåller förslag till hur nämnda direktiv ska genomföras i svensk rätt.

I Regeringskansliet arbetar man för närvarande med att ta fram en nationell strategi för informations- och cybersäkerhet, som tar sin utgångspunkt i det förslag som lades fram i betänkandet *Informations- och cybersäkerhet i Sverige*.[3] Planen är att strategin ska presenteras under sommaren 2017.

Vidare publicerar Enisa, EU:s nätverks- och informationssäkerhetsbyrå, löpande studier och rekommendationer för att förbättra informationssäkerheten i samhället.

Även andra internationella organ ger rekommendationer om informationssäkerhet, som exempelvis OECD och FN.[4]

På standardiseringsområdet finns det flera olika initiativ för att systematisera och harmonisera arbetet med cyber- och informationssäkerhet.

12.2.2 Informationssäkerhet i dataskyddsförordningen

Dataskyddsförordningen ställer en rad krav på såväl tekniska som organisatoriska informationssäkerhetsåtgärder. Vissa av dessa krav finns redan i dataskyddsdirektivet, medan andra är nya:

- Personuppgiftsbiträden får ett eget ansvar för informationssäkerheten även när de behandlar uppgifter enligt instruktion från den personuppgiftsansvarige (artikel 32.1).

[2] SOU 2017:36.
[3] Betänkande av NISU 2014, *Informations- och cybersäkerhet i Sverige*, (SOU 2015:23).
[4] En detaljerad förteckning över internationella organisationer på området och hur de arbetar, finns i betänkandet *Informations- och cybersäkerhet i Sverige* (SOU 2015:23).

- Det införs en anmälningsskyldighet för personuppgiftsincidenter (artikel 33).
- Uttryckliga krav införs på inbyggt dataskydd och dataskydd som standard (artikel 25).
- Viss precisering görs (i förhållande till dataskyddsdirektivet) av de allmänna kraven på säkerhet i samband med behandlingen (artikel 32).
- Det införs en skyldighet att göra konsekvensbedömningar avseende dataskydd (artikel 35).
- Dataskyddsombudets roll i övervakningen av efterlevnaden av dataskyddsreglerna förtydligas och ändras delvis (artikel 39.1). Det föreskrivs vidare att dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbiträdets högsta förvaltningsnivå (artikel 38.3).

12.2.3 Tillsyn

Integritetskommitténs förslag: Regeringen bör vidta de utredningsåtgärder som är nödvändiga för att genomföra det förslag som lämnades i SOU 2015:23 om att Myndigheten för samhällsskydd och beredskap (MSB) ska utöva tillsyn över statliga myndigheters informationssäkerhetsarbete.

I betänkandet *Informations- och cybersäkerhet i Sverige*[5] föreslogs att tillsynen över den statliga sektorns informationssäkerhet skulle samordnas och förstärkas, genom att MSB ges i uppgift att bedriva tillsyn över statliga myndigheters arbete med informationssäkerhet.

Bakgrunden till förslaget var såväl konstaterade brister i statliga myndigheters informationssäkerhet som den splittrade tillsynen, som innebär att ingen myndighet har ett helhetsperspektiv med samtidig möjlighet till tillsyn. Förslaget bereds ännu inom Regeringskansliet.

Integritetskommittén anser utifrån sin kartläggning i delbetänkandet, att behovet av mer och bättre tillsyn över statliga myndig-

[5] SOU 2015:23.

heters informationssäkerhet snarast har ökat sedan MSB föreslogs få ett tillsynsansvar i betänkandet från år 2015.

Kommittén anser därför att regeringen bör vidta de utredningsåtgärder som är nödvändiga för att genomföra förslaget om tillsynsansvar för MSB över den statliga sektorns informationssäkerhet. I arbetet bör beaktas bland annat att Datainspektionen i sitt remissvar på det aktuella betänkandet uppmärksammat att förslaget inte innehöll några tillsynsbefogenheter för MSB (exempelvis skyldighet för myndigheterna att lämna uppgifter till MSB).[6] Eftersom förslaget lämnats relativt nyligen, bör de utredningsinsatser som kan bli aktuella för Regeringskansliet i den här frågan, rimligen vara mindre omfattande.

I dag är statliga myndigheter skyldiga att anmäla it-incidenter till MSB. När dataskyddsförordningen ska börja tillämpas kommer alla myndigheter, företag och organisationer att behöva anmäla personuppgiftsincidenter till Datainspektionen. Vi anser att det är av stor betydelse hur både MSB och Datainspektionen agerar när de får in anmälningarna. Förutom att inleda tillsyn i vissa fall, är det önskvärt att bägge myndigheterna sammanfattar och publicerar detaljerade rapporter och analyser rörande de inkomna anmälningarna. Detta i syfte att med största möjliga transparens möjliggöra att personuppgiftsansvariga kan lära av andras misstag och att de kan vidta konkreta åtgärder för att förbättra skyddet för sina data och sina system. Sådana rapporter skulle också utgöra ett bra beslutsunderlag för regeringen i det fortsatta arbetet med att förstärka samhällets informationssäkerhet. Vi menar att MSB och Datainspektionen i detta arbete kan få viss ledning från arbetet med olyckor inom luft- och sjöfarten, där Statens haverikommission granskar inträffade olyckor i syfte att komma fram till vad som kan göras för att en liknande händelse inte ska inträffa i framtiden, eller i syfte att minska konsekvenserna om händelsen inträffar igen.

[6] Datainspektionens remissyttrande den 15 september 2015 i dnr 934-2015.

12.2.4 Uppföljning av statliga myndigheter

Integritetskommitténs förslag: Regeringen bör uppdra åt MSB att beträffande myndigheter under regeringen följa upp vilka åtgärder myndigheterna vidtar för att följa kraven i MSB:s föreskrifter (MSBFS 2016:1) om statliga myndigheters informationssäkerhet.

I delbetänkandet redovisas en rad olika brister i statliga myndigheters informationssäkerhetsarbete. Intrycket av att det behövs åtgärder för att förbättra arbetet, har sedermera stärkts genom MSB:s sammanställning över myndigheternas incidentrapportering till MSB, Säkerhetspolisen och Försvarsmakten.[7] I sammanställningen framgår bland annat att MSB bedömer att det som rapporterats inte ligger i paritet med det verkliga antalet allvarliga it-incidenter. Bland de inrapporterade incidenterna, är störning i driftmiljö och angrepp de vanligaste incidentkategorierna. Vidare framgår att bland dem som har drabbats av infektioner i it-system, har de myndigheter som haft en god ordning på sin it-verksamhet fått mindre störningar än de som inte haft lika bra kontroll över sin it-verksamhet.

Mot denna bakgrund, anser kommittén att regeringen närmare bör följa vilka åtgärder som statliga myndigheter vidtar i syfte att förbättra informationssäkerheten och integritetsskyddet.

Förslagsvis ges MSB i uppdrag att genomföra en uppföljning av vilka åtgärder myndigheterna vidtar i detta hänseende. Inledningsvis kan uppföljningen ta sikte på vilka åtgärder myndigheterna vidtagit för att följa kraven i MSB:s föreskrifter (MSBFS 2016:1)om statliga myndigheters informationssäkerhet.

MSB:s uppföljning kan antingen avse alla myndigheter under regeringen, eller endast avse ett urval av sådana myndigheter som hanterar känsliga personuppgifter eller stora mängder av personuppgifter.

I sin återrapportering av uppdraget bör MSB även rekommendera åtgärder ner på myndighetsnivå. Regeringen bör, med utgångspunkt i MSB:s rekommendationer, i respektive myndighets regleringsbrev

[7] MSB:s *Årsrapport It-incidentrapportering 2016*, daterad den 14 mars 2017 med dnr 2016-6304-7.

ålägga myndigheten att vidta vissa åtgärder i informationssäkerhetsarbetet.

En lämplig, om än inte nödvändig, förutsättning för ett uppföljningsuppdrag av detta slag, är att MSB ges det tillsynsmandat som tidigare föreslagits och som kommittén anser nu bör genomföras.

12.2.5 Uppförandekoder

Integritetskommitténs bedömning: De insatser för att åstadkomma uppförandekoder som kommittén föreslår i andra avsnitt i detta betänkande, bör innehålla informationssäkerhetsåtgärder som framträdande inslag. Om insatserna förverkligas, kan de innebära en generell förbättring av förutsättningarna för en bättre informationssäkerhet i samhället.

På en rad områden föreslår kommittén i detta betänkande att regeringen genom sina myndigheter ska initiera och stödja de personuppgiftsansvarigas och personuppgiftsbiträdenas arbete med att ta fram uppförandekoder för sina respektive områden. Som framgår i de områdesspecifika avsnitten i detta betänkande, kan uppförandekoderna i enlighet med dataskyddsförordningens artikel 40.2 h innehålla specificeringar bland annat av vilka åtgärder som krävs inom de olika branscherna för att säkerställa säkerhet vid behandling i enlighet med dataskyddsförordningens artikel 32, dvs. informationssäkerhetsåtgärder.

Vi föreslår att regeringen ska initiera och stödja framtagandet av uppförandekoder inom konsumentområdet, skolan, hälso- och sjukvården, arbetslivet och e-förvaltningen. Informationssäkerhetsåtgärder bör utgöra ett framträdande inslag i samtliga dessa koder.

När det gäller informationssäkerhet och dataskydd inom hälso- och sjukvårds- samt socialtjänstområdet föreslår kommittén att staten tar ett särskilt ansvar genom att en myndighet får i uppdrag att vara sekretariat för arbetet med att ta fram och förvalta en uppförandekod för dessa integritetskänsliga verksamheter (kapitel 7).

Om arbetet med koder blir verklighet, kan det innebära en generell förbättring av förutsättningarna för olika aktörer i samhället, både offentliga och privata, att förbättra sin informationssäkerhet.

12.2.6 En nationell styrmodell

Integritetskommitténs förslag: Regeringen bör ge MSB i uppdrag att i samverkan med andra myndigheter utveckla, förvalta och vidareutveckla en styrmodell för statens informationssäkerhet, i enlighet med det som föreslagits i SOU 2015:23.

I betänkandet *Informations- och cybersäkerhet i Sverige*[8] efterlyses en nationell satsning på systematiskt informationssäkerhetsarbete i statlig verksamhet. Utredningen föreslog därför att ett gemensamt ramverk, en nationell styrmodell, för statens informationssäkerhetsarbete ska etableras:

> Genom denna ska ett för de statliga myndigheterna gemensamt förhållningssätt till informationssäkerhetsfrågor säkerställas. Styrmodellen blir en gemensam bas för statligt informationssäkerhetsarbete. Utredningens förslag avser i första hand de statliga myndigheterna och ska vara normerande för dessa men styrmodellen kan på sikt utsträckas till att omfatta hela den offentliga sektorn.

En gemensam styrmodell syftar enligt betänkandet till att myndigheters informationssäkerhetsarbete ska utföras på ett enhetligt sätt. Syftet är också att skapa en gemensam syn på en grundskyddsnivå av informationssäkerhet i staten och samtidigt att höja denna från dagens situation i vissa verksamheter. Det ska alltså skapas en samlad modell innefattande bland annat gemensamma metoder för inventering av informationstillgångar, riskanalys, riskhantering, informationsklassning, avbrotts- och kontinuitetshantering, definierade skyddsnivåer med tillhörande skyddsåtgärder, gemensamma kravbilder och säkerhetsnivåer, terminologi för informationssäkerhetsarbete och regelverk. Styrmodellen ska enligt betänkandet baseras på existerande krav i författningar och verksamheternas behov.

Enligt förslaget ska MSB vara den myndighet som bör få i uppdrag att utveckla, förvalta och vidareutveckla styrmodellen.

Utifrån de risker rörande informationssäkerheten hos myndigheterna som konstaterades i delbetänkande, och utifrån de nya krav på informationssäkerhet som uppställs i dataskyddsförordningen, delar kommittén bedömningen att det behövs en nationell styr-

[8] SOU 2015:23.

modell för informationssäkerhet i samhället på sätt som föreslogs i SOU 2015:23. Vi föreslår därför att regeringen genomför detta förslag.

13 Samhällets skyddsmekanismer

13.1 Problemet

Integritetskommittén gjorde i delbetänkandet bedömningen att den fysiska eller juridiska person som gör sig skyldig till ett otillbörligt intrång i någon annans personliga integritet, löper liten risk att råka ut för någon sanktion, vare sig av tillsynsmyndigheten, genom någon ersättningsskyldighet eller något straff. Den som drabbas av intrånget får inte någon ersättning som motsvarar den upplevda kränkningen. Sanktionssystemet har på så sätt inte den kompensatoriska och den preventiva effekt som är önskvärd.

Det allmänna har ett ansvar för att skydda enskildas privatliv och integritet. De skyddsmekanismer som kommittén undersökte i delbetänkandet var:

- Tillsyn
- Ekonomisk ersättning
- Straffrättsliga sanktioner

En ytterligare faktor, som påverkar enskildas möjligheter att skydda sig mot intrång i den personliga integriteten är:

- Den enskildes kunskap om digitaliseringen och dess effekter på den personliga integriteten.

Tillsyn

Kommittén har bedömt att omfattningen av tillsynen inom området inte är tillräckligt stor för att säkerställa skyddet för behandlade personuppgifter på ett önskvärt sätt.

Kommitténs bedömningar och förslag som gäller tillsynsmyndigheten finns i kapitel 14.

Ekonomisk ersättning

Kommittén har bedömt att de olika formerna av ekonomisk kompensation som finns, inte används i sådan omfattning som vore önskvärt för att skydda och kompensera enskilda för otillåtet intrång i den personliga integriteten. Företag, myndigheter eller enskilda personer som begår ett otillåtet intrång i andras personliga integritet, löper en mycket liten risk att behöva ersätta den skadelidande för intrånget. Vi anser därtill att de belopp som betalas ut ofta är låga.

Kommittén har bedömt att det är svårt för enskilda att över huvud taget veta vart de ska vända sig för att få kompensation för en kränkning. Enskilda avhåller sig också från att driva skadeståndsärenden på grund av att den ekonomiska risken är stor. Det ingår därtill inte i Datainspektionens uppdrag att bistå enskilda i mål om skadestånd vid allmän domstol.

Straffrättsliga sanktioner

Kommittén har bedömt att de straffrättsliga sanktionerna inte heller används i sådan omfattning som vore önskvärt. Den som begår ett otillåtet intrång i andras personliga integritet, löper mycket liten risk att råka ut för någon straffrättslig sanktion. Detta, i kombination med låga straffsatser och att de bakomliggande regelverken (bland annat personuppgiftslagen och registerförfattningarna) är relativt komplicerade, minskar möjligheten till lagföring och skadestånd. Internetrelaterad brottslighet ställer krav på både specialistkompetens och tillräckliga resurser hos polis och åklagare.

13.2 Åtgärder för att stärka skadeståndsrätten som rättsmedel

Integritetskommitténs förslag: Regeringen bör låta utreda frågan om Datainspektionen ska ges i uppdrag att som part föra talan i domstol, för en enskild som medger det, i utvalda ersättningsärenden.

13.2.1 Rätt att driva enskildas skadeståndsärenden

När en enskild person utsätts för intrång i sin personliga integritet är det svårt för honom eller henne att tillvarata sina rättigheter. Bestämmelserna om hur personuppgifter får hanteras är komplicerade och utgör till stora delar av ramlagstiftning, som måste fyllas ut av rättstillämpningen. Regelverket för ekonomisk kompensation är också svårtillgängligt. Därtill är riskerna med att inleda en rättslig process stora, om det inte är ett mål som går att driva som ett förenklat tvistemål.[1] Detta medför att det kan vara svårt för en enskild person att ta till vara sina rättigheter.

Datainspektionen förfogar över specialistkunskap rörande rättsläget avseende tillämpningen av integritetsskyddslagstiftningen. Genom sin sakkunskap har myndigheten unika förutsättningar att överblicka behovet av vägledande avgöranden inom området och driva ett målinriktat arbete med att stärka rättsutvecklingen. En möjlighet för Datainspektionen att föra talan i principiellt viktiga mål i domstol skulle underlätta för myndigheten att fullgöra sitt uppdrag att på olika sätt motverka integritetskränkningar.[2]

Integritetskommittén anser därför att förutsättningarna för att införa en rätt för Datainspektionen att i vissa fall av integritetskränkningar företräda enskilda i domstol bör utredas.

Det finns redan andra myndigheter som har liknande uppgifter att företräda enskilda som lidit skada, exempelvis Konsumentverket, Diskrimineringsombudsmannen och Barn- och elevombudet vid Skolinspektionen.

[1] Yrkandet om ersättning ska då enligt 1 kap. 3 d § rättegångsbalken vara lägre än ett halvt basbelopp.
[2] Datainspektionen har efterlyst att en sådan möjlighet för myndigheten utreds, se Datainspektionens skrivelse till regeringen den 9 december 2011 (Datainspektionens dnr 1760-2011).

Syftet med att på detta sätt utöka även Datainspektionens verktyg är främst att ge möjlighet för myndigheten att ta initiativ till att driva ärenden och skapa praxis inom områden där sådan saknas. Det är alltså inte fråga om att inrätta en allmän ombudsmannafunktion för enskilda som har anspråk på skadestånd. Kommittén bedömer att detta skulle kunna bli en alltför resurskrävande arbetsuppgift för Datainspektionen, vars främsta prioritet bör vara den aktiva tillsynen. Däremot anser vi att ett praxisskapande arbete skulle gynna både tillsynsverksamheten och skyddet för den personliga integriteten. Även andra enskilda än den som Datainspektionen valt att företräda kan dra nytta av att myndigheten driver principiellt viktiga ärenden.

Kommittén anser att de kriterier som bör ligga till grund för valet av ärenden som Datainspektionen ska driva, behöver utredas närmare och därmed bör omfattas av utredningsuppdraget. Utöver principiellt viktiga ärenden kan det finnas andra urvalskriterier. Datainspektionen bör kanske också kunna företräda en enskild i ärenden som avser intrång som har drabbat ett mycket stort antal andra enskilda på ett mycket kränkande sätt. Det kan kanske också vara så att det finns ömmande skäl för att myndigheten ska företräda den enskilde. Vi anser att en utredning bör få i uppdrag att utreda under vilka förutsättningar som Datainspektionen ska få företräda enskilda i tvister om ersättning för integritetsintrång.

Regeringen har därtill möjlighet att ge Datainspektionen i uppdrag att företräda en grupp av enskilda med stöd av lagen (2002:599) om grupprättegång. Enligt 6 § denna lag får offentlig grupptalan väckas av en myndighet som med hänsyn till vad tvisten rör är lämpad att företräda gruppmedlemmarna. Det är regeringen som bestämmer vilka myndigheter som får väcka offentlig grupptalan.

I kapitel 14 om tillsynsmyndigheten kommenterar vi på vilka sätt och på vilka grunder lagstiftaren kan styra Datainspektionens arbetsuppgifter. I dataskyddsförordningens artikel 58.6 anges dessutom att varje medlemsstat i lagstiftning får föreskriva att dess tillsynsmyndighet ska ha ytterligare befogenheter utöver dem som avses i punkterna 1, 2 och 3 i artikel 58. Utövandet av dessa ytterligare befogenheter ska enligt dataskyddsförordningen inte påverka den effektiva tillämpningen av förordningens kapitel VII. Förordningens kapitel VII rör samarbete och enhetlighet mellan medlemsstaternas tillsynsmyndigheter. Rätten till skadestånd framgår av dataskyddsförordningens artikel 82 som är placerad i förordningens kapitel VIII. En

möjlighet i lag för Datainspektionen att som part föra talan i domstol för enskilda, bör därför anses som förenlig med förordningens artikel 58.6. En sådan möjlighet skulle förstärka enskildas rätt till skadestånd, och kan på så sätt anses bidra till ett starkt integritetsskydd, vilket är ett av de grundläggande syftena med förordningen. En möjlighet av detta slag för Datainspektionen skulle också bidra till att stärka enskildas rätt enligt artikel 79 till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde.

13.2.2 Ersättningsnivåerna

Ersättningsnivån när det gäller skadestånd bestäms av praxis. Det är därför svårt att påverka storleken på de belopp som domstolarna dömer ut.

Det finns dock exempel på att lagstiftaren gjort vissa försök att påverka ersättningsbelopp. I diskrimineringslagen finns exempelvis möjlighet att ta hänsyn till preventiv effekt vid bestämmande av ersättning.

Enligt diskrimineringslagen ska den som bryter mot förbuden mot diskriminering eller repressalier eller som inte uppfyller sina skyldigheter att utreda och vidta åtgärder mot trakasserier eller sexuella trakasserier, betala diskrimineringsersättning för den kränkning som överträdelsen innebär. När ersättningen bestäms ska därför särskilt syftet att motverka sådana överträdelser av lagen beaktas. Ersättningen ska betalas till den som kränkts av överträdelsen.

Överträdelser av diskrimineringslagstiftningen ska enligt förarbetena[3] därför ses som en allvarlig kränkning:

> När diskriminering förekommit, ska påföljden vara kännbar för den skyldige. Regeringen anser att den nya diskrimineringslagen bör skapa förutsättningar för kraftfulla och avskräckande påföljder vid diskriminering. Valet av påföljd bör ske med utgångspunkt i detta ställningstagande. I nuvarande diskrimineringslagar har skadestånd valts som påföljd vid överträdelser av lagstiftningen. Skadeståndet har här en dubbel funktion; det ska dels ge kompensation åt den som drabbas, dels avhålla från överträdelser. Genom denna preventiva funktion fyller skadestånd vid diskriminering delvis andra ändamål än vanligt skadestånd. Vid skadestånd med anledning av brott uppfylls den preventiva funktionen även av de påföljder som föranleds av brottet i fråga, t.ex.

[3] Regeringens proposition, *Ett starkare skydd mot diskriminering*, prop. 2007/08:95, s. 390.

> fängelse eller böter för den skyldige. I de flesta fall av överträdelser av den svenska diskrimineringslagstiftningen är skadeståndet däremot den enda preventiva sanktion som förekommer vid dessa kränkningar.

I NJA 2014 s. 499 I och II uttalade sig Högsta domstolen om hur denna regel i diskrimineringslagen ska förstås. Högsta domstolen konstaterade att ersättningen i diskrimineringsersättningssammanhanget fyller en dubbel funktion. Den ska ersätta den kränkning som diskrimineringen innebär men samtidigt också avskräcka från diskriminering. Båda dessa funktioner påverkar ersättningens bestämmande. Högsta domstolen delade upp ersättningen i två komponenter: Upprättelseersättning och preventionspåslag. När det gäller upprättelsekomponenten kan ersättningens bestämmande utgå från den praxis som vuxit fram under skadeståndslagens regel i 2 kap. 3 §. Preventionspåslaget ska enligt domstolen normalt kunna uppskattas till samma belopp som upprättelseersättningen, även om det finns utrymme att avvika uppåt och nedåt. Lägsta diskrimineringsersättning blir således i regel 10 000 kronor, i jämförelse med att lägsta kränkningsersättningsbelopp under skadeståndslagens regel är 5 000 kronor. Genom Högsta domstolens avgöranden, får alltså diskrimineringsersättningens preventiva funktion en framträdande roll.

Enligt 48 § i nu gällande personuppgiftslag ska den personuppgiftsansvarige ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med lagen har orsakat.

Från och med den 25 maj 2018 kommer i stället motsvarande rätt till ersättning att gälla direkt enligt artikel 82 i dataskyddsförordningen. Varje registrerad som anser att hans eller hennes rättigheter enligt förordningen har åsidosatts till följd av att personuppgifter har hanterats på ett sätt som inte är förenligt med förordningen har enligt artikel 79 rätt till ett effektivt rättsmedel.

Vi kan konstatera att även när det gäller integritetskränkande brott är straffrättsliga påföljder ovanliga. Skadestånd skulle därför även inom detta område kunna ha en viktigt preventiv funktion. En tänkbar åtgärd vore därför att låta utreda möjligheten att komplettera dataskyddsförordningen med en bestämmelse i svensk lag om att beakta det preventiva syftet när ersättningsbeloppet bestäms. Det skulle kunna möjliggöra en ersättning som i likhet med diskrimineringsersättning består av två komponenter; upprättelseersättning och preventionspåslag.

Vid bedömningen av hur ersättningen i så fall skulle bestämmas anser kommittén att det allmänna intresset av att motverka integritetskränkningar genom brott mot dataskyddsförordningen borde ha särskild betydelse.[4] Detta innebär att ersättningen generellt skulle kunna bestämmas till så höga belopp att påföljden effektivt verkar avhållande från överträdelser. När det gäller överträdelser som begås i näringsverksamhet borde en sådan bestämmelse innefatta en möjlighet att beakta exempelvis omsättningen i verksamheten. I en verksamhet med hög omsättning torde det i normalfallet krävas ett högre ersättningsbelopp för att den avskräckande effekten ska uppnås. En annan faktor som kunde inverka är i vilken mån tidigare överträdelser av dataskyddsförordningen förekommit i verksamheten. En sådan bestämmelse skulle enligt kommittén ligga i linje med dataskyddsförordningens krav på effektiva rättsmedel.

Vi bedömer dock att en utredning av frågan om att komplettera förordningen enligt resonemanget ovan kan anstå till dess att dataskyddsförordningen har varit ikraft under några år och effekterna av förändringarna bättre kan överblickas.

Något om ersättningsreglerna i dataskyddsförordningen

Enligt förordningens artikel 82.1 ska varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av förordningen ha rätt till ersättning från den personuppgiftsansvarige för den uppkomna skadan. En nyhet i förordningen är att även personuppgiftsbiträden kan bli skadeståndsskyldiga under vissa förutsättningar. I skäl 146 och i artikel 82.2–5 preciseras närmare under vilka förutsättningar personuppgiftsansvariga och personuppgiftsbiträden kan hållas ansvariga för uppkomna skador. Bland annat anges där att varje personuppgiftsansvarig som medverkat vid behandlingen ska ansvara för uppkommen skada. Det stadgas också att den personuppgiftsansvarige ska undgå ansvar om den visar att den inte på något sätt är ansvarig för den händelse som orsakade skadan. Sammantaget leder detta tanken till att ett i princip strikt skadeståndsansvar gäller enligt förordningen för såväl ekonomisk som ideell skada, dvs. en liknande

[4] Jfr prop. 2007/08:95, s. 554.

reglering som den som gäller enligt personuppgiftslagen. Den närmare innebörden av bestämmelserna får dock utvecklas i rättspraxis.

Förordningen innebär också ett förtydligande jämfört med det nu gällande direktivet, genom att varje personuppgiftsansvarig eller personuppgiftsbiträde som har medverkat vid en behandling, kan hållas ansvarig för hela skadan, dvs. att ett solidariskt ansvar gäller när det finns flera personuppgiftsansvariga eller personuppgiftsbiträden för samma behandling.

Sanktionerna ska enligt dataskyddsförordningen vara effektiva, proportionella och avskräckande.

En annan möjlighet för den skadelidande som regleras i förordningen är rätten att företrädas av en organisation. Enligt artikel 80 dataskyddsförordningen har den registrerade rätt att ge ett organ, en organisation eller sammanslutning utan vinstsyfte, i uppdrag att bland annat lämna in ett klagomål till tillsynsmyndigheten (i Sverige Datainspektionen) för hans eller hennes räkning och att utöva den rätt till ersättning som avses i artikel 82, under förutsättning att det också föreskrivs i medlemsstatens nationella rätt. Organisationen i fråga ska ha inrättats på lämpligt sätt i enlighet med lagen i medlemsstaten. Kommittén bedömer att bestämmelsen kan sägas innebära ett tydliggörande av den ordning som redan gäller i svensk rätt, enligt vilken exempelvis en person i en ideell förening, med fullmakt från enskilda kan företräda dessa i förhållande till förvaltningsmyndigheter och domstolar genom att ge in klagomål eller stämningsansökningar.[5]

Såvitt kommittén känner till finns det i dagsläget i Sverige endast ett fåtal föreningar av detta slag, såsom Institutet för internet och juridik samt Centrum för rättvisa.

[5] Kravet på att det ska vara en fysisk person som anges i fullmakten gäller redan i dag för mål i domstolarna, och föreslås gälla även i ärenden hos förvaltningsmyndigheter, se prop. 2016/17:180 *En modern och rättssäker förvaltning – ny förvaltningslag*, s. 90 f.

13.3 Åtgärder för att förbättra det straffrättsliga sanktionssystemet

Integritetskommitténs förslag: Datainspektionen bör i sin årliga redovisning till regeringen redogöra för i vilken mån rättsmedlen är effektiva för att skydda registrerades rättigheter.

Regeringen bör följa upp att polis och åklagare följer de rekommendationer avseende kompetens och metod för utredning av it-relaterad brottslighet som Riksrevisionen har rekommenderat och redovisa resultatet av uppföljningen till riksdagen.

13.3.1 Rapportering om det straffrättsliga sanktionssystemet i den årliga redovisningen

I delbetänkandet föreslog Integritetskommittén att Datainspektionens uppdrag att följa och beskriva utvecklingen på it-området när det gäller frågor som rör personlig integritet och ny teknik, ska utvidgas till att även omfatta de legala förutsättningarna för integritetsskyddet och att myndigheten årligen ska lämna en redovisning om utvecklingen inom området till regeringen.[6] Kommittén föreslog även att Datainspektionen ska få ökade resurser för detta uppdrag.[7] Vi anser att det är naturligt att det i denna uppgift ingår att analysera om rättsmedlen är tillräckligt effektiva för att skydda enskilda och om de uppfyller dataskyddsförordningens kvalitetskrav.

Kommittén anser att de administrativa sanktionsavgifter som införs genom dataskyddsförordningen och pågående lagstiftningsarbeten inom straffrätten innebär steg i rätt riktning för att stärka den enskilde i samband med integritetskränkningar. Det är viktigt att Datainspektionen följer utvecklingen och ger regeringen signaler om det behövs ytterligare åtgärder.

I kapitel 14 om tillsynsmyndigheten kommenterar vi på vilka sätt och på vilka grunder regeringen kan styra Datainspektionens uppgifter.

[6] SOU 2016:41, s. 641 ff.
[7] SOU 2016:41, s. 657 ff.

13.3.2 Ändamålsenlig och effektiv utredning av it-relaterad brottslighet

I delbetänkandet redogjorde Integritetskommittén för brister avseende lagföring av it-relaterad brottslighet som såväl Brottsförebyggande rådet[8] och Riksrevisionen[9] har rapporterat. Båda myndigheterna identifierade brister i kompetens avseende denna typ av brottslighet hos polis och åklagare.

Riksrevisionens rapport utmynnade i följande rekommendationer till Polismyndigheten:

- Identifiera nationella utvecklingsbehov och utveckla den strategiska kompetensförsörjningen för att kunna säkerställa verksamhetens behov. Planera, uppmuntra och skapa utrymme för kompetenshöjande åtgärder inom it-området.
- Säkerställ att grundutbildningen till polis motsvarar verksamhetens behov med hänsyn till den tekniska utvecklingen och dess påverkan på brottsligheten.
- Utveckla och förankra nationella arbetssätt och metodstöd för utredning av it-relaterade brott.
- Se över strukturen för brottssamordning och samverkan mellan polisregionerna.
- Utnyttja de fora som finns för internationell samordning och samverkan.

Och följande rekommendationer till Åklagarmyndigheten

- Identifiera nationella utvecklingsbehov och utveckla den strategiska kompetensförsörjningen för att kunna säkerställa verksamhetens behov. Planera, uppmuntra och skapa utrymme för kompetenshöjande åtgärder inom it-området.
- Utveckla och förankra metodstödet inom it-området och möjligheterna till erfarenhetsutbyte mellan åklagarområdena

[8] *Polisanmälda hot och kränkningar mot enskilda personer via internet*, Rapport 2015:6.
[9] *It-relaterad brottslighet – polis och åklagare kan bli effektivare*, RiR 2015:21.

Av regeringens rapport[10] till riksdagen över Riksrevisionens rapport framgår att regeringen noggrant följer Polismyndighetens och Åklagarmyndighetens arbete på området och har inlett en dialog med myndigheterna om de rekommendationer som Riksrevisionen har lämnat till myndigheterna. Regeringen överväger att vid behov begära närmare redovisning av hur Riksrevisionens rekommendationer tas om hand.

Justitieutskottet anför i sitt betänkande[11] över Riksrevisionens rapport att utskottet ser positivt på att regeringen har inlett en dialog med dessa myndigheter om rekommendationerna och att man överväger att vid behov begära närmare redovisning av hur rekommendationerna tas om hand.

Kommittén ansluter sig till dessa bedömningar och betonar vikten av att regeringen genom att begära redovisning från Polismyndigheten följer upp att dessa åtgärder vidtas så att polis och åklagare kan utreda it-relaterade brott mer effektivt. Detta kan som regeringen anfört i sin rapport göras till exempel genom att begära redovisning från de berörda myndigheterna. Resultatet av denna uppföljning bör redovisas för riksdagen.

13.3.3 Administrativa sanktionsavgifter enligt dataskyddsförordningen

Dataskyddsförordningen kommer att erbjuda andra möjligheter än rent straffrättsliga när det gäller felaktig behandling av personuppgifter genom de nya sanktionsavgifterna.

Sanktionsavgifterna införs enligt skäl 148 för att stärka verkställigheten av förordningen. Bestämmelserna om administrativa sanktionsavgifter återfinns i artikel 83 och i förordningens skäl 148 till och med 150.

Av artikel 83.1 framgår att det är den nationella tillsynsmyndigheten som ska besluta om sanktionsavgifter vid överträdelser av förordningens bestämmelser. I artikel 83.2 finns en detaljerad reglering av vilka faktorer som ska beaktas vid beslut om sanktionsavgifter och bestämmande av avgiftens storlek. Bland annat ska tillsynsmyndig-

[10] Regeringens skrivelse 2015/16:164.
[11] 2015/16:JuU27.

heten vid beslutet beakta överträdelsens karaktär, svårighetsgrad och varaktighet, samt om överträdelsen varit uppsåtlig eller oaktsam. Det är alltså inte ett uttryckligt krav i förordningstexten att överträdelsen ska ha gjorts med uppsåt eller oaktsamhet för att sanktionsavgift ska bli aktuellt, men subjektiva omständigheter hos den personuppgiftsansvarige är en faktor som ska beaktas.

Andra faktorer som tillsynsmyndigheten ska beakta är antalet berörda registrerade, vilken skada de har lidit, om den personuppgiftsansvarige har försökt förebygga eller i efterhand komma till rätta med överträdelsen och eventuell ekonomisk vinst som görs eller ekonomisk förlust som undviks genom överträdelsen.

För överträdelser av vissa regler i förordningen, exempelvis dem om inbyggt dataskydd, förteckningar och konsekvensbeskrivningar, fastslås ett maxbelopp på 10 000 000 euro eller 2 procent av den globala årsomsättningen om det gäller ett företag, beroende på vilket belopp som är högst. För överträdelser av vissa andra regler, exempelvis dem om de grundläggande principerna för behandling och om rätten till information, rättelse och radering, fastslås ett maxbelopp om 20 000 000 euro eller 4 procent av den globala årsomsättningen. Dataskyddsutredningen har föreslagit att sanktionsavgifter även ska kunna påföras statliga och kommunala myndigheter.[12]

Administrativa sanktionsavgifter kommer på grund av de höga beloppen som anges i bestämmelserna sannolikt att utgöra ett starkt incitament för personuppgiftsansvariga och personuppgiftsbiträden att se över sin personuppgiftshantering.

13.3.4 Budapestkonventionen

Europarådets it-brottskonvention CETS no. 185 (Budapestkonventionen) syftar huvudsakligen till att harmonisera lagstiftning och förenkla internationellt samarbete gällande cyberbrottslighet. Konventionen avser att fastlägga riktlinjer för nationell lagstiftning på området samt vara ett ramverk för internationellt samarbete mellan de stater som har ratificerat den. Sverige undertecknade Budapestkonventionen 2001 men har ännu inte ratificerat den. Vissa före-

[12] Dataskyddsutredningens betänkande *Ny dataskyddslag – kompletterande bestämmelser till EU:s dataskyddsförordning*, (SOU2017:39).

trädare för de brottsutredande myndigheterna menar att det skulle underlätta det internationella samarbetet om Sverige ratificerade konventionen.

Det finns ett betänkande[13] avseende Sveriges tillträde till konventionen. Det har remitterats och nu pågår inom Regeringskansliet arbete med en lagrådsremiss.

13.3.5 Andra befintliga förslag till att stärka den straffrättsliga regleringen

I betänkandet Integritet och straffskydd[14] föreslås en ny straffbestämmelse om olaga integritetsintrång, som innebär ett straffansvar för den som gör intrång i någon annans privatliv genom att sprida bild eller annan uppgift på ett sätt som syftar till att medföra kännbar skada för den som uppgiften rör. Utredaren föreslår också en rad förtydliganden av befintliga straffbestämmelser i brottsbalken till skydd för den personliga integriteten. Dessutom föreslår utredningen att rätten till brottsskadeersättning ska utvidgas till vissa ärekränkningsbrott. Förslaget bereds inom Regeringskansliet och en proposition är planerad att läggas fram under året.

13.4 Åtgärder för att förbättra den enskildes kunskaper

Integritetskommitténs förslag: Regeringen bör ge en myndighet i uppdrag att utreda hur en nationell folkbildningsinsats bör vara organiserad och utformad samt vilken omfattning och finansiering en sådan insats bör ha.

Digitaliseringen av samhället och den förändring av vårt sätt att leva och kommunicera som den för med sig, skulle i viss mån kunna jämföras med högertrafikomläggningen – även om digitaliseringen inne-

[13] Utredningens om it-brottskonventionens betänkande *Europarådets konvention om it-relaterad brottslighet, (*SOU 2013:39).
[14] Utredningens om ett modernt och starkt straffrättsligt skydd för den personliga integriteten betänkande *Integritet och straffskydd,* (SOU 2016:7).

bär en betydligt mer genomgripande samhällsförändring. Jämförelsen ska därför inte drivas allt för långt.

Däremot kan det informationsarbete som fördes i samband med högertrafikomläggningen kunna vara en förebild för hur genomgripande samhällets insats behöver vara. Övergången till högertrafik innebar en förändring av samspelet i trafiken, som påverkade hela samhället. En förändring som krävde kunskapshöjande åtgärder riktade till enskilda individer för att omställningen skulle kunna genomföras på ett säkert sätt. Sannolikt behöver dock folkbildningen i ett digitaliserat samhälle bedrivas över en betydligt längre tid.

För att planera och genomföra högertrafikomläggningen inrättades en särskild myndighet; Statens högertrafikkommission, som ansvarade för förberedelsearbetet. Det gällde exempelvis att anpassa vägnätet samt bussar, spårvagnar och vissa andra fordon till den nya trafikriktningen. Men den viktigaste delen av förberedelsearbetet gällde trafiksäkerheten och ”ombyggnaden av trafikanterna”. Målsättningen var att varje trafikant måste nås med information om att högertrafik skulle införas, när den skulle införas och hur man skulle uppträda i trafiken. Dessutom måste alla som färdades på gator och vägar få veta vad som skulle göras inför trafikomläggningen och ta del av de nya bestämmelserna. För att nå detta mål drevs en informationskampanj som förmodligen var den största som någonsin genomförts i Sverige.[15]

Integritetskommittén gör bedömningen att digitaliseringen innebär stora utmaningar för oss som enskilda individer. Den påverkar vårt sätt att leva och interagera med andra människor. När vi lever vårt nya digitala liv lämnar vi elektroniska spår bakom oss. Dessa spår har ett ekonomiskt värde och kan användas på en mängd olika sätt och för olika syften. Detta medför konsekvenser som är svåra att överblicka. Regeringen har en vision för samhällets digitalisering. För att vi ska kunna närma oss den visionen på ett säkert sätt bedömer kommittén att regeringen också måste ta ansvar för att medborgarna är rustade för denna omställning.

Regeringen har formulerat målsättningen att Sverige ska vara bäst i världen på att utnyttja digitaliseringens möjligheter. Kommittén delar Medieutredningens bedömning att det krävs en omfattande och långsiktig satsning på medie- och informationskunnighet (MIK), rik-

[15] Vägverket, Vägverkets museum, Jan-Erik Montelius, 2004-11-12.

tad till samtliga medborgare för att nå detta mål.[16] MIK definieras som de förmågor som gör att en människa kan finna, analysera, kritiskt värdera och själv skapa information i olika medier och kontexter.[17] Utöver denna kompetens avseende informationshantering behöver individen också kunskap och insikter om på vilket sätt den personliga integriteten påverkas av informationsanvändningen. Medieutredningen beskriver kunskapsbehovet på detta sätt:

> I en tid av hastiga förändringar på området uppstår behov av att, i takt med teknikutvecklingen, iterativt arbeta med kunskapsmålen. När informationsinhämtning inte längre handlar om att använda ett traditionellt medium utan i allt högre utsträckning börjar med en sökning i en sökmotor behöver kraven också omtolkas och anpassas. Begrepp som källkritik t.ex. bör utvecklas till att omfatta algoritmkritik. Färdigheter i medieanvändning bör t.ex. även omfatta medvetenhet om hur varje delning skapar digitala fotspår, men också hur användningen över tid utgör en slags mediediet, som varje medborgare behöver balansera.[18]

Kunskapshöjande åtgärder avseende digitaliseringens effekter på den personliga integriteten är särskilt viktiga för barn och ungdomar. Barn och unga är ofta vana användare av ny teknik, men den yngre generationen kommer på ett mer genomgripande sätt än äldre att utsättas för en rad olika integritetsrisker genom hela livet och i takt med att samhället blir allt mer digitaliserat. Kunskapshöjande insatser måste därför utformas av befintliga myndigheter med ansvar för barn, unga, skola och en trygg uppväxt. En myndighet med ett sådant uppdrag är Statens medieråd som enligt sin instruktion bland annat ska verka för att stärka barn och unga som medvetna medieanvändare i syfte att skydda dem mot skadlig mediepåverkan.

När det gäller äldre medborgare finns naturligtvis också ett stort behov av grundläggande kunskap om digitaliseringen.

Kommittén anser därför att flera olika myndigheter bör få i uppdrag att inom sitt ansvarsområde utforma och bedriva omfattande folkbildning avseende digitaliseringen och dess inverkan på den personliga integriteten. Vi anser att den myndighet som får det samlade ansvaret för den offentliga förvaltningens digitalisering, samt Konsumentverket, Skolverket, Statens medieråd, Datainspektionen och andra myndigheter och organisationer i civilsamhället borde vara

[16] Medieutredningens slutbetänkande *En gränsöverskridande mediepolitik*, (SOU 2016:80).
[17] SOU 2016:80, s. 407.
[18] SOU 2016:80, s. 410.

självklara aktörer inom detta område. Dessa måste samarbeta med varandra för att utforma folkbildningsinsatsen på ett så bra och verkningsfullt sätt som möjligt. De folkbildande aktiviteterna bör även syfta till att öka den enskildes kunskaper om hur man tar tillvara sin rätt i samband med integritetskränkningar.

Regeringen bör inledningsvis ge en myndighet i uppdrag att utreda på vilket sätt en nationell folkbildningsinsats bör vara organiserad och utformad samt vilken omfattning och finansiering en sådan insats bör ha för att få avsedd effekt.

14 Tillsynsmyndigheten

14.1 Riskerna

14.1.1 För lite tillsyn

I delbetänkandet konstaterade kommittén att Datainspektionen på senare år successivt har minskat sina tillsynsaktiviteter.

Kommittén gjorde bedömningen att tillsynen är mycket viktig. Nya företeelser introduceras i en mycket snabb takt. Många av dessa finns det anledning att bedöma ur ett rättsligt perspektiv. Regelverket är tämligen oprecist och avsiktligt allmänt hållet. Det är därför ofta först när tillsynsmyndigheten har bedömt en ny företeelse, som leverantörer och andra användare får någon ledning. Resultatet från tillsynen kan sedan användas i tillsynsmyndighetens utåtriktade och proaktiva arbete för att sprida kunskap.

I Datainspektionens årsredovisning för år 2016 framgår att antalet inledda och avslutade tillsynsärenden under 2016 fortsatt ligger på en låg nivå i förhållande till tidigare år. Vidare kan noteras att Datainspektionen ägnar mer och mer tid åt att delta i kommittéarbete och svara på remisser – år 2016 ägnades nästan lika mycket tid åt detta arbete, som åt att utöva tillsyn enligt personuppgiftslagen.[1]

Kommittén har naturligtvis förståelse för att förberedelsearbetet med anledning av den nya dataskyddsförordningen kan medföra en tillfällig nedgång av omfattningen av tillsynsverksamheten.

[1] För kommittéarbete och remisser redovisades 6 744 timmar, för tillsyn enligt personuppgiftslagen 7 509 timmar.

14.1.2 För lite resurser

Datainspektionen gör i årsredovisningen för år 2016 bedömningen att det anslag som tilldelats myndigheten för år 2017 är helt otillräckligt för att Datainspektionen ska kunna fungera som tillsynsmyndighet enligt dataskyddsförordningen och dataskyddsdirektivet. Datainspektionen lämnade därför i januari 2017 ett kompletterande budgetunderlag till Justitiedepartementet med äskande om ytterligare anslag, vilket myndigheten anser vara helt avgörande för att den ska kunna fullfölja sitt nya uppdrag enligt dataskyddsförordningen.

14.1.3 För lite vägledning

I delbetänkandet konstaterade kommittén att flera myndigheter efterlyser mer vägledning från tillsynsmyndigheten i samband med digitaliseringen av förvaltningen. Även i flera av remissvaren på vårt delbetänkande framförs önskemål om tydligare och mer konkret vägledning från Datainspektionen i frågor som rör integritetsskydd.

Vi anser att inspiration till ett utåtriktat och konsultativt arbetssätt med fördel kan hämtas från andra tillsynsmyndigheter i vårt närområde.

Norge

I norska Datatilsynets årsredovisning för år 2014 framgår att myndigheten lägger stor vikt vid arbetet med kommunikation och vägledning, och att myndigheten därför använder nästan en fjärdedel av sina personalresurser till detta, det vill säga omkring tio årsarbetskrafter. I denna del av Datatilsynets verksamhet inräknas myndighetens tekniska och juridiska vägledningsarbete, utbildningsverksamhet, mediakontakter och annan kommunikationsverksamhet. I sina årsredovisningar följer Datatilsynet upp sitt resultat i vägledningsoch kommunikationsarbetet, exempelvis redovisar myndigheten hur många inlägg och följare som myndigheten haft på Twitter under året. Datatilsynet redovisar även hur ofta myndigheten omnämns i media. Vidare låter Datatilsynet utvalda medarbetare blogga om aktuella företeelser. På eget initiativ har Datatilsynet de senaste åren tagit fram en framåtriktad temarapport i samarbete med norska

Teknologirådet. Det kan också noteras att Datatilsynet deltar som observatör i styrgruppen för Norm for informasjonssikkerhet, en norsk uppförandekod för hälso- och sjukvård och omsorg (läs mer i kapitel 7).

Sammanfattningsvis kan Datatilsynet sägas ha ett väl fungerande vägledning- och kommunikationsarbete, med det tydliga syftet att belysa och lyfta frågor om integritetsskydd i olika former och sammanhang. Det är värt att notera att Datatilsynet utför sitt samlade uppdrag med ett anslag som inte stort skiljer sig från Datainspektionens i Sverige.

Storbritannien

I Storbritannien publicerar dataskyddsmyndigheten Information Commissioner's Office (ICO) utkast till sin verksamhetsplan på webben, och uppmanar allmänheten att lämna synpunkter på vad man anser att ICO ska arbeta med.

ICO utför även s.k. *advisory visits*, som innebär att företag och organisationer (inte myndigheter) bjuder in ICO som sedan lämnar rekommendationer för ett förbättrat dataskydd. Syftet med dessa besök är bland annat att hitta goda exempel som ska kunna spridas genom ICO:s försorg.

Frankrike

I Frankrike har dataskyddsmyndigheten Commission Nationale de l'Informatique et des Libertés (CNIL) under 2016 och 2017 bett allmänheten om synpunkter på vilken slags vägledning man anser sig behöva från CNIL och Artikel 29-gruppen i förberedelsearbetet inför dataskyddsförordningen.

14.1.4 Integritetskommitténs iakttagelser

Kommittén anser att tillsynsmyndighetens arbetssätt är viktigt, inte bara när det gäller tillsynen. Det är även viktigt att myndigheten har förutsättningar och resurser för att arbeta proaktivt och lösningsfokuserat, och kan erbjuda samverkan och samråd med företag och myndigheter.

Här vilar självklart ett primärt ansvar hos personuppgiftsansvariga företag och myndigheter att vända sig till Datainspektionen när tvekan uppstår kring hur integritetsskyddet tillgodoses i den egna verksamheten.

14.1.5 Nya krav enligt dataskyddsförordningen

När dataskyddsförordningen ska börja tillämpas den 25 maj 2018, inträder en lång rad nya och obligatoriska arbetsuppgifter för Datainspektionen. I sitt budgetunderlag för 2017–2019 har Datainspektionen identifierat bland annat följande nya arbetsuppgifter:

- En skyldighet att samarbeta med andra dataskyddsmyndigheter inom EU, till exempel i form av gemensamma tillsynsåtgärder och skyldighet att ge andra dataskyddsmyndigheter bistånd i tillsynsärenden.
- Bestämmelserna om gränsöverskridande behandling innebär att det i varje tillsynsärende måste utredas om behandlingen är gränsöverskridande och om det finns någon annan behörig dataskyddsmyndighet som ska involveras i tillsynsarbetet.
- En skyldighet att medverka i Europeiska dataskyddsstyrelsen, som genom förordningen får ett omfattande uppdrag bland annat genom mekanismen för enhetlighet och tvistelösning i tillsynsärenden.
- Ta fram en lista för vilka behandlingar av personuppgifter som den personuppgiftsansvarige ska göra en konsekvensbedömning avseende dataskydd.
- Lämna samrådsyttrande inom åtta veckor till den personuppgiftsansvarige i de fall dennes konsekvensbedömning indikerar att behandlingen innebär hög risk.

- Utföra förhandskontroller och lämna tillstånd i de fall den svenska lagstiftaren beslutar om detta.
- Uppmuntra utarbetandet av uppförandekoder, yttra sig över förslag till sådana och publicera godkända uppförandekoder samt om de gäller gränsöverskridande behandling överlämna till Europeiska dataskyddsstyrelsen att yttra sig.
- Uppmuntra tillkomsten av certifieringsmekanismer och sigill och märken för personuppgiftsbehandling samt regelbundna utvärderingar av sådana.
- Ta fram kriterier för ackreditering av certifieringsorgan och organ för övervakning av uppförandekoder.
- Ta emot och hantera anmälningar om personuppgiftsincidenter från personuppgiftsansvariga.
- Medverka till internationellt samarbete med länder utanför EU och internationella organisationer i större utsträckning än för närvarande.

14.2 Åtgärder

14.2.1 Regeringens möjligheter att styra Datainspektionen

Enligt artikel 8 i EU:s stadga om de grundläggande rättigheterna är kontrollen av en oberoende myndighet en del av den grundläggande rätten till skydd för personuppgifter.

Enligt dataskyddsförordningen ska varje tillsynsmyndighet vara fullständigt oberoende i utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med förordningen. Varje tillsynsmyndighets ledamot eller ledamöter ska också i utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med förordningen stå fria från utomstående påverkan, direkt såväl som indirekt, och får varken begära eller ta emot instruktioner av någon. Vidare åligger det enligt dataskyddsförordningen varje medlemsstat att säkerställa att varje tillsynsmyndighet förfogar över de personella, tekniska och finansiella resurser samt de lokaler och den infrastruktur som behövs för att myndigheten ska kunna utföra sina uppgifter och utöva sina befogenheter, även inom ramen för det ömse-

sidiga biståndet, samarbetet och deltagandet i den europeiska dataskyddsstyrelsens verksamhet.[2]

Frågan om vad dessa krav innebär för Sveriges del, berörs av Utredningen om tillsynen över den personliga integriteten.[3] I dess betänkande anförs bland annat följande.

> Den svenska förvaltningsmodellen innebär starka och till största delen grundlagsfästa garantier för oberoende i beslutsfattandet för förvaltningsmyndigheter under regeringen. De kommande EU-rättsakternas krav på tillsynsmyndighetens oberoende uppfylls enligt vår mening utan tvekan med den svenska ordningen. Det kan tilläggas att redan det nu gällande dataskyddsdirektivet ställer krav på att tillsynsmyndigheterna ska vara fullständigt oberoende.[4]

När det emellertid kommer till innehållet i förordningen (2007:975) med instruktion för Datainspektionen, sägs i betänkandet följande.

> Dataskyddsförordningen är direkt tillämplig i medlemsstaterna och Datainspektionen ska därför direkt på grundval av förordningen ha de uppgifter som följer av denna reglering. Det saknas därför behov av att härutöver reglera dessa uppgifter i myndighetsinstruktionen. Vi ser heller inte något behov av att av andra skäl föreslå några kompletterande bestämmelser i instruktionen om Datainspektionens uppgifter. Härtill torde förordningens tydliga krav på tillsynsmyndigheternas oberoende göra att utrymmet för regeringen att styra Datainspektionen genom regleringar i myndighetsinstruktionen generellt är begränsat.[5]

Vi anser att det även efter den 25 maj 2018 i viss utsträckning kommer att vara möjligt för regeringen att i regeringsuppdrag, regleringsbrev eller myndighetens instruktion ge uppdrag till Datainspektionen. Frågan om sådana uppdrag är förenliga med dataskyddsförordningens krav på självständighet får bedömas från fall till fall.

En generell förutsättning för att det ska vara möjligt att ge sådana uppdrag, är att Datainspektionen tillförs tillräckliga medel för uppdragets utförande. Att myndigheten får särskilda anslag för att utföra ett visst uppdrag, innebär att uppdragets utförande inte minskar myndighetens möjligheter och resurser för att på ett självständigt sätt utföra sina övriga arbetsuppgifter enligt dataskyddsförordningen.

---

[2] Artikel 52 i dataskyddsförordningen.
[3] Utredningens om tillsynen över den personliga integriteten betänkande, *Ett samlat ansvar för tillsyn över den personliga integriteten* (SOU 2016:65).
[4] *Ett samlat ansvar för tillsyn över den personliga integriteten* (SOU 2016:65) sid. 146.
[5] *Ett samlat ansvar för tillsyn över den personliga integriteten* (SOU 2016:65) sid. 160.

Regeringens uppdrag får naturligtvis inte heller komma i konflikt med 12 kap. 2 § regeringsformen som slår fast att ingen myndighet, inte heller riksdagen eller en kommuns beslutande organ, får bestämma hur en förvaltningsmyndighet i ett särskilt fall ska besluta i ett ärende som rör myndighetsutövning mot en enskild eller mot en kommun eller som rör tillämpningen av lag.

Bestämmelserna i dataskyddsförordningen om tillsynsmyndighetens oberoende bör ses i ljuset av förhållandena i vissa andra medlemsstater, där förvaltningen är en del av regeringens kansli och där den ansvariga ministern kan utöva ett direkt bestämmande över myndigheterna.

Det är mot ovanstående, samlade bakgrund som Integritetskommittén i delbetänkandet har ansett sig kunna föreslå att regeringen genom en ändring i Datainspektionens instruktion ska reglera vilka frågor som myndigheten särskilt ska återrapportera till regeringen. Förslaget innefattar även en anslagsökning som beräknas motsvara den ökade arbetsinsats som vårt förslag skulle innebära. Datainspektionens oberoende ställning innebär att det därutöver står myndigheten fritt att i sin rapportering till regeringen även beskriva andra aspekter av sin verksamhet eller andra företeelser och händelser i omvärlden, även inkluderande exempelvis regeringens agerande i olika ärenden.

Här kan jämföras med hur regeringen genom förordningen (2000:605) om årsredovisning och budgetunderlag, som även riktar sig till Datainspektionen, bestämmer vilket innehåll som årsredovisningen ska ha, samt när och till vem den ska lämnas.

För det fall att regeringen ändå inte skulle anse sig ha möjlighet att i enlighet med kommitténs förslag styra Datainspektionen genom myndighetens instruktion, har regeringen fortsatt möjlighet att styra myndigheten i regleringsbrev eller särskilda regeringsuppdrag – under tidigare nämnda förutsättningar.

För det fall att regeringen skulle anse att även detta styrsätt är oförenligt med dataskyddsförordningen, kvarstår för regeringen endast möjligheten att genom överläggningar, överenskommelser och delvis villkorade anslag, stimulera myndigheten att företa vissa åtgärder, utöver det myndigheten redan gör med finansiering genom sitt grundanslag. Ett sådant arbetssätt kan jämföras med hur regeringen förhåller sig till exempelvis organisationen Sveriges kommuner och landsting (SKL) i vissa frågor, där regeringen kan ingå över-

enskommelser med SKL om att SKL ska utföra viss verksamhet som regeringen sedan helt eller delvis finansierar.

14.2.2 Analysera Datainspektionens arbetssätt och behov av anslag

Integritetskommitténs förslag: Regeringen bör ge Statskontoret i uppdrag att utföra en myndighetsanalys av Datainspektionen enligt den modell som Statskontoret redovisade till regeringen i december 2008 i rapporten *Modell för myndighetsanalyser* (2008:17).

Kommittén delar Datainspektionens oro för att myndighetens beviljade anslag inte kommer att räcka till för att på ett tillfredsställande sätt fullgöra alla myndighetens skyldigheter enligt dataskyddsförordningen. Datainspektionen kommer att få många nya arbetsuppgifter, den kommer att behöva samverka mer både nationellt och internationellt, samtidigt som samhället i och med dataskyddsförordningen kommer att behöva mycket mer stöd och vägledning. Parallellt med denna utveckling kommer Datainspektionen, på samma sätt som alla andra myndigheter, att behöva utveckla och förbättra sin verksamhet och sina arbetssätt.

Vidare har det sannolikt inte sedan Datainspektionen bildades år 1973 genomförts någon riktigt grundläggande analys av myndighetens samlade resursbehov i förhållande till sitt uppdrag. En ytlig jämförelse av olika tillsynsmyndigheters bemanning visar på stora skillnader. Exempelvis har Konsumentverket cirka 170 anställda, Livsmedelsverket 530, Post- och telestyrelsen 260, Skolinspektionen 400, Diskrimineringsombudsmannen 90, Säkerhets- och integritetsskyddsnämnden 20 och Datainspektionen cirka 50 anställda. Det är, enligt uppgift, cirka 30 fler än då Datainspektionen startade år 1973. Samtidigt har myndighetens arbetsfält genomgått enorma förändringar sedan 1973.

Vi anser sammanfattningsvis att det är mycket svårt att enbart på grundval av Datainspektionens årsredovisning och kompletterande budgetäskande bedöma hur stort anslaget till myndigheten behöver vara under kommande år för att myndigheten ska klara av sina nya arbetsuppgifter.

För att klargöra vilket anslag, vilka resurser och vilka kompetenser, som Datainspektionen behöver de närmaste åren, anser vi att regeringen bör ge Statskontoret i uppdrag att utföra en myndighetsanalys av Datainspektionen enligt den modell som Statskontoret redovisade till regeringen i december 2008 i rapporten *Modell för myndighetsanalyser* (2008:17). Statskontorets analys bör belysa bland annat följande punkter:

- hur Datainspektionen fullgör sitt uppdrag enligt sin instruktion,
- hur interna faktorer och omvärldsfaktorer påverkar Datainspektionens möjligheter att fullgöra sitt uppdrag, samt beskriva interna faktorer och omvärldsfaktorer av särskild vikt för Datainspektionens möjligheter att fullgöra sitt uppdrag framöver,
- hur Datainspektionens samverkan med andra aktörer fungerar,
- vilka faktorer som är av särskild betydelse för effektiviteten i verksamheten, och
- identifiera områden som Datainspektionen eller regeringen behöver utveckla för att Datainspektionen ska kunna fullgöra sitt uppdrag framöver, samt föreslå hur detta bör göras.

Myndighetsanalysen ska utgöra ett led i ambitionen att ge Datainspektionen optimala förutsättningar att leva upp till de möjligheter och utmaningar som dataskyddsförordningen innebär, och till de förväntningar som finns på prestationer och effekter inom området.[6]

En myndighetsanalys enligt nämnda modell innefattar en systematisk metod för extern analys av en myndighet med syftet att utveckla och stödja arbetet med den årliga resultatstyrningen och bredda regeringens bedömningsunderlag.[7]

Kommittén vill betona att en sådan myndighetsanalys har en annan inriktning och ett annat syfte än det uppdrag som regeringen gav åt Utredningen om tillsynen över den personliga integriteten och som avrapporterades i september 2016 genom betänkandet *Ett samlat ansvar för tillsyn över den personliga integriteten*.[8] I betänkandet

[6] Det förekommer även att myndigheter själva ber om en myndighetsanalys av Statskontoret, exempelvis för att kunna påvisa ett behov av ökade anslag.
[7] Statskontorets rapport *Modell för myndighetsanalyser* (2008:17).
[8] SOU 2016:65.

föreslås i huvudsak att Datainspektionen ska vara tillsynsmyndighet enligt dataskyddsförordningen samt att en ändring ska göras av anställningsformen för Datainspektionens chef. Vidare lämnas förslag till mindre ändringar i gränsdragningen mellan tillsynsansvaret hos Datainspektionen, Säkerhets- och integritetsskyddsnämnden respektive Post- och telestyrelsen.

15 Forskning om personlig integritet

15.1 Problemen

15.1.1 Forskning om inverkan på människor och samhället

En bilaga till vårt delbetänkande utgjordes av en systematisk kunskapsöversikt över forskning om på vilket sätt människans beteende påverkas av förändringar i den privata sfären och av den accelererande digitala hanteringen av personuppgifter. Översikten, som tagits fram av Lunds universitet, visar att det såväl internationellt som i Sverige finns förvånansvärt lite kunskap om vilken inverkan som digital övervakning har på människans beteende och uppfattning om världen och sig själv.

Översikten visar att det råder en tämligen strikt indelning av forskningen om digitalisering och personlig integritet mellan huvudsakligen tre vetenskapliga fält. Det första är ett tekniskt fält som i hög grad handlar om systemutveckling. Det andra är ett juridiskt fält med fokus på frågor om författningsskydd för den personliga integriteten. Det tredje är ett mer allmänt samhällsvetenskapligt fält som samlar bl.a. informatik, psykologi, marketing och managementforskning.

Gemensamt för alla tre fälten är att forskare inom respektive fält endast sällan visar intresse för vad som görs inom något av de andra fälten. Något annat som också framkommit är att det, i forskning som rör personlig integritet, saknas en gemensam begreppsapparat och gemensamma metoder för de olika vetenskapliga fälten och disciplinerna.

Iakttagelserna i översikten kan hjälpa till att förklara varför problemställningar som förekommer inom juridiken (exempelvis att uppgifter hanteras för nya ändamål som är oförenliga med de ursprungliga ändamål för vilka uppgifterna samlades in) inte i högre utsträckning hämtar idéer till lösningar från teknikfältet (exempelvis att uppgifterna anonymiseras på ett sätt som minimerar integritets-

riskerna utan att försämra möjligheten att få ny kunskap ur datasamlingen).

I det här kapitlet lämnar Integritetskommittén förslag till åtgärder för att öka kunskapen om på vilket sätt människan påverkas av förändringar i den privata sfären och av den accelererande digitala hanteringen av personuppgifter.

15.1.2 Användningen av integritetsskyddande teknik

En fråga som ligger nära forskningen, är användandet av integritetsskyddande teknik. I delbetänkandet uppmärksammade kommittén att integritetsskyddande teknik skulle kunna användas i betydligt större omfattning än vad som är fallet i dag.

Vi gav en informationssäkerhetspecialist i uppdrag att ta fram en översikt över integritetsskyddande teknik, vilken ingick som en bilaga till delbetänkandet.

I översikten tas flera goda exempel upp. Översikten har som utgångspunkt bland annat att användningen av väl utformad integritetsfrämjande teknik gör det möjligt att uppnå en mer fördelaktig jämvikt i avvägningen mellan nyttoeffekter och risker för den personliga integriteten.

15.2 Förslag till åtgärder

15.2.1 Stöd till forskning

Integritetskommitténs förslag: Regeringen bör ge Vetenskapsrådet i uppdrag att fördela anslag till tvärvetenskaplig forskning om på vilket sätt människan påverkas av förändringar i den privata sfären och av den accelererande digitala hanteringen av personuppgifter.

Det behövs mer kunskap

Integritetskommittén anser att regeringen, riksdagen, myndigheterna samt många företag och organisationer behöver ett bättre kunskapsunderlag för att kunna fatta välgrundade beslut och kunna göra långsiktiga bedömningar när det gäller samhällets digitalisering.

Digitaliseringen är enligt kommitténs uppfattning av så avgörande betydelse för samhällets framtida utveckling, att regeringen omgående bör investera i forskning för att förbättra kunskapsläget. Exempelvis bör ökad kunskap ge bättre förutsättningar för regeringens satsning på att digitalisera förvaltningen, i synnerhet som digitaliseringen av den offentliga förvaltningen ofta har ett ensidigt fokus på effektivisering och lägre kostnader.

Sådan forskning bör vara tvärvetenskaplig och vara inriktad frågan om på vilket sätt människan påverkas av förändringar i den privata sfären och av den accelererande digitala hanteringen av personuppgifter.

Ett tvärvetenskapligt forskningsinstitut

En möjlighet att åstadkomma mer forskning är att regeringen finansierar inrättandet och driften av ett nytt, tvärvetenskapligt forskningsinstitut med inriktning på personlig integritet. Ett övergripande villkor för finansieringen kan då vara att forskningen bedrivs tvärvetenskapligt.

Ett sådant instituts självständighet kan sägas utgöra såväl en styrka som en svaghet. Institutet är inte bundet av någon annan myndighets bedömningar eller instruktioner, utan kan självständigt formulera frågeställningar och utveckla egna metoder utan att begränsas av några utomstående intressen eller styrgrupper. Det innebär emellertid även att någon löpande extern styrning av verksamheten i syfte att garantera exempelvis tvärvetenskapligheten, inte är möjlig.

Ett exempel på forskningsinstitut med tvärvetenskaplig inriktning är Internetsinstitutet vid Lunds universitet.

Inrättandet av ett självständigt forskningsinstitut är ett kostsamt alternativ, eftersom det innebär fasta kostnader för löner, lokaler, utrustning m.m.

En myndighet som fördelar forskningsanslag

En annan möjlighet att åstadkomma mer forskning är att regeringen ger en myndighet på området i uppdrag att fördela anslag till forskningsprojekt om personlig integritet med tvärvetenskaplig inriktning hos olika forskningshuvudmän. Förslaget förutsätter att regeringen ger den utvalda myndigheten anslag att fördela till forskningsprojekt.

Styrkan med denna modell är att myndigheten kan se till att varje projekt som beviljas medel har en tvärvetenskaplig prägel. Vidare kan myndigheten styra forskningen till frågor som är relevanta för myndighetens uppdrag. Svagheten hos modellen ligger i att forskningshuvudmännen blir mindre fria att själva formulera forskningsfrågor, vilket kan leda till att forskningens inriktning blir alltför snäv och inriktad på myndighetens egna intressen.

Exempel på myndigheter som fördelar forskningsanslag är Kronofogden, MSB och Konsumentverket.[1] Dessa myndigheter har vetenskapliga råd knutna till sig, som har till uppgift att bedöma vilka projekt som ska få stöd. Det är en förutsättning för detta alternativ att den ansvariga myndigheten knyter vetenskaplig kompetens till sig, för att kunna bedöma projektens vetenskaplighet och de sökande forskarnas kompetens.

Vetenskapsrådet

En annan möjlighet att åstadkomma mer forskning är att via Vetenskapsrådet fördela forskningsanslag som öronmärks för tvärvetenskaplig forskning om på vilket sätt människan påverkas av förändringar i den privata sfären och av den accelererande digitala hanteringen av personuppgifter.

Vetenskapsrådet är Sveriges största externa finansiär av forskning inom universitets- och högskolesektorn. Myndigheten har även i uppgift att göra forskningspolitiska analyser, utvärdera forskning och ge regeringen forskningspolitiska råd.

En betydande del av Vetenskapsrådets finansiering består av stöd till vetenskapliga projekt där forskare själva formulerat frågeställ-

[1] Av särskilt intresse i detta sammanhang, är att MSB bl.a. finansierar forskning om informationssäkerhet.

ningar och utarbetat metoder för att besvara dessa. För att kunna ge dessa forskningsstöd har Vetenskapsrådet flera olika anslag från regeringen. Dessutom finansierar Vetenskapsrådet forskningsinfrastruktur, forskningsmiljöer, forskarskolor, olika former av samverkan samt medlemskap i internationella organisationer och större forskningsanläggningar.[2]

För sina prövningar av ansökningar om anslag, anlitar Vetenskapsrådet cirka 800 aktiva forskare, svenska eller utländska, med expertkunskaper inom olika områden. Vetenskapsrådets beredningsgrupper bedömer och prioriterar varje år drygt 6 000 ansökningar efter vetenskaplig kvalitet och de sökandes kompetens. Hos Vetenskapsrådet finns således en väl fungerande organisation redan på plats för att bedöma vetenskaplighet och kompetens.

Det förekommer att regeringen ger Vetenskapsrådet i uppdrag att finansiera forskning med viss inriktning. Två exempel på detta är ett flervetenskapligt grundforskningsprogram om det civila samhället och ett forskningsprogram inom området rasism.[3] Vetenskapsrådet ombesörjer i dessa fall utlysningar och prövningar av individuella ansökning till programmen.

Integritetskommitténs bedömning

Kommittén förordar alternativet att ge Vetenskapsrådet i uppdrag att fördela forskningsanslag som öronmärks för tvärvetenskaplig forskning om på vilket sätt människan påverkas av förändringar i den privata sfären och av den accelererande digitala hanteringen av personuppgifter.

Kommittén är av uppfattningen att detta alternativ både ger störst möjlighet att uppnå bra forskningsresultat och kostar mindre än de andra alternativen.

Det finns en risk om regeringen alltför detaljerat styr forskningens inriktning: En alltför snäv inriktning och detaljerad styrning kan innebära att konkurrensen om att få utföra forskningen minskar, eftersom avgränsningen begränsar antalet forskare som kan komma i fråga. Om det endast är ett mindre antal forskare som visar intresse

[2] Vetenskapsrådets årsredovisning 2015.
[3] Regleringsbrev för budgetåret 2017 avseende Vetenskapsrådet.

för området, finns det en risk för att forskningen blir smalare och att resultaten påverkas negativt. Det är därför viktigt att regeringen inte ytterligare avgränsar forskningens inriktning, jämfört med det förslag som lämnas här.

Beträffande storleken på de forskningsmedel som Vetenskapsrådet bör få i uppdrag att fördela, anser vi att ledning kan sökas i liknande satsningar som regeringen genomfört med hjälp av Vetenskapsrådet. Exempelvis har regeringen givit Vetenskapsrådet i uppdrag att från och med 2016 fördela minst 20 miljoner kronor för att stärka forskning inom området rasism.[4] Vidare har regeringen givit Vetenskapsrådet i uppdrag att genomföra ett flervetenskapligt grundforskningsprogram om det civila samhället för vilket Vetenskapsrådet under 2017 disponerar 14 miljoner kronor totalt.[5]

Med utgångspunkt i dessa satsningars storlek, och utifrån bedömningen att det behövs mer kunskap för att kunna genomföra digitaliseringen av samhället på bästa möjliga sätt för individen, anser vi att Vetenskapsrådet som ett engångsbelopp bör få disponera mellan 14 och 20 miljoner kronor för forskning om på vilket sätt människan påverkas av förändringar i den privata sfären och av den accelererande digitala hanteringen av personuppgifter.

15.2.2 Integritetsskyddande teknik och arbetssätt

Integritetskommitténs förslag: Regeringen bör ge Vinnova i uppdrag att främja projekt som involverar integritetsskyddande teknik och arbetssätt.

Regeringen bör även ge Vinnova i uppdrag att upplysa om dataskyddsförordningen och att i verkets arbete med att finansiera och på andra sätt främja forskning och utveckling ställa krav utifrån dataskyddsförordningens regler.

[4] Regeringsuppdrag U2016/00588/F.
[5] Regleringsbrev för budgetåret 2017 avseende Vetenskapsrådet.

Det är kommitténs uppfattning att användningen av väl utformad integritetsskyddande teknik borde öka generellt i samhället och på olika sätt stödjas av det allmänna.

Förutom att det finns outnyttjade möjligheter att stärka integritetsskyddet utan negativa effekter på användbarhet och effektivitet, kommer dataskyddsförordningen att ställa nya krav på användning av integritetsskyddande teknik och arbetssätt, bland annat dessa:

- Uttryckliga krav införs på inbyggt dataskydd och dataskydd som standard (artikel 25).
- Viss precisering görs (i förhållande till dataskyddsdirektivet) av de allmänna kraven på säkerhet i samband med behandlingen (artikel 32).
- Det införs en skyldighet att göra konsekvensbedömningar avseende dataskydd (artikel 35).

Även de nya kraven i dataskyddsförordningen talar således för att det allmänna i större utsträckning än i dag bör sysselsätta sig med integritetsskyddande teknik och arbetssätt.

Ett sätt för regeringen att bidra till utvecklingen, är att ge Vinnova (Verket för innovationssystem) i uppdrag att främja användningen av integritetsskyddande teknik och arbetssätt.

Vinnova har enligt sin instruktion till uppgift att främja hållbar tillväxt genom finansiering av behovsmotiverad forskning och utveckling av effektiva innovationssystem.[6] Myndigheten har ett särskilt ansvar inom teknikområdet samt områdena transport, kommunikation och arbetsliv. Med innovationssystem avses nätverk av offentliga och privata aktörer där ny teknik och kunskap produceras, sprids och används. Myndigheten ska även verka för nyttiggörande av forskning för att uppnå hållbar tillväxt och stärka Sveriges konkurrenskraft.

Vinnova utför sitt uppdrag bland annat genom att finansiera forskning och utveckling av effektiva innovationssystem. Varje år investerar Vinnova cirka 2,7 miljarder kronor i finansiering av olika insatser.

[6] Förordningen (2009:1101) med instruktion för Verket för innovationssystem.

Kommittén anser att regeringen bör ge Vinnova i uppdrag att främja sådana projekt som involverar integritetsskyddande teknik och arbetssätt. Regeringen bör även ge Vinnova i uppdrag att upplysa om dataskyddsförordningen och att i verkets arbete med att finansiera och på andra sätt främja forskning och utveckling ställa krav utifrån dataskyddsförordningens regler.

16 Uppföljning av grundlagsskyddets effekt i lagstiftningsarbetet

16.1 Uppdraget

Integritetskommittén ska inom ramen för kartläggningsuppdraget även följa upp och analysera effekterna i lagstiftningsarbetet av den förstärkning av grundlagsskyddet för den personliga integriteten, som infördes genom lagstiftning som trädde i kraft 2011.

Den förstärkning som avses här, är bestämmelsen i 2 kap. 6 § andra stycket regeringsformen (RF). Bestämmelsen stadgar att var och en är skyddad gentemot det allmänna mot betydande intrång i den personliga integriteten som sker utan samtycke och innebär kartläggning eller övervakning av enskilds personliga förhållanden.

16.1.1 Bakgrunden till det förstärkta integritetsskyddet i regeringsformen

Regeringen beslutade i april 2004 om direktiv till en parlamentarisk kommitté, Integritetsskyddskommittén[1], med uppdrag att kartlägga och analysera sådan lagstiftning som rör den personliga integriteten, att överväga om regeringsformens bestämmelse om skydd för den personliga integriteten borde ändras samt att överväga om det vid sidan av befintlig lagstiftning borde finnas generellt tillämpliga bestämmelser till skydd för den personliga integriteten.

Kartläggnings- och analysuppdraget redovisades i betänkandet *Skyddet för den personliga integriteten – Kartläggning och analys*.[2]

[1] Ju 2004:05.
[2] SOU 2007:22.

I sitt slutbetänkande *Skyddet för den personliga integriteten – Bedömningar och förslag*[3] redovisade kommittén bl.a. förslag till ett stärkt grundlagsskydd för den personliga integriteten.

Integritetsskyddskommittén kunde efter genomförd kartläggning konstatera att rättighetsbegränsande lagstiftning ofta arbetades fram utan att konsekvenserna för integritetsskyddet beaktades tillräckligt[4]. Kommittén framhöll att en lagstiftning av hög kvalitet måste vara baserad på genomtänkta behovsanalyser, intresseavvägningar och konsekvensbeskrivningar. Kännetecken på en sådan lagstiftning är ändamålsenlighet, lagtekniskt invändningsfria lösningar, lättillgänglighet och klarhet. Den förutsätter ett fullvärdigt beslutsunderlag, noggrant arbete och tillräckligt med tid. Kommittén framhöll att det får en rad negativa konsekvenser om kvaliteten i lagstiftningen eftersätts. Det kan leda till att skyddsbehov av olika slag inte uppmärksammas eller får för liten uppmärksamhet i förhållande till andra intressen. Det kan också leda till att lagstiftningen blir osammanhängande, motsägelsefull och mindre väl förenlig med sitt syfte. Alla dessa slag av kvalitativa tillkortakommanden hade kommittén påträffat vid sin kartläggning av den svenska integritetsskyddslagstiftningen.[5]

Integritetsskyddskommitténs slutsats var att grundlagsskyddet för den personliga integriteten behövde stärkas. När det gällde frågan hur detta skulle åstadkommas hade kommittén funnit det nödvändigt att utgå från den uppbyggnad som fri- och rättighetsskyddet redan hade i regeringsformen. Det innebar att ett utökat skydd inte borde utformas som en positiv förpliktelse för det allmänna, exempelvis i form av ett stadgande som ålägger det allmänna att visa respekt för varje medborgares rätt till personlig integritet. Skyddet måste i stället utformas som ett förbud för lagstiftaren, dvs. riksdagen, att vidta integritetsbegränsande åtgärder, såvida inte begränsningarna gjordes i form av lagstiftning som var underkastad det i regeringsformen särskilt föreskrivna förfarandet vid rättighetsbegränsande lagstiftning.[6]

Resultatet av Integritetsskyddskommitténs kartläggning och analys gav enligt regeringens uppfattning belägg för slutsatsen att lagstiftning som innefattar intrång i den enskildes personliga integritet i

[3] SOU 2008:3.
[4] SOU 2007:22 s. 445 ff.
[5] SOU 2008:3 s. 189.
[6] SOU 2008:3 s. 16.

viss utsträckning uppvisade brister.[7] Regeringen hänvisade till de brister som kommittén funnit, bl.a. att de avvägningar mellan olika motstående intressen som normalt ska göras i lagstiftningsärenden i vissa fall var bristfälligt redovisade. Regeringen återgav också kommitténs påpekande att det i första hand var de negativa effekterna av olika integritetsbegränsande åtgärder som var knapphändigt belysta. Det kunde enligt regeringens uppfattning inte uteslutas att detta förhållande kan ha fått negativa återverkningar för enskilda i den meningen att det kan ha påverkat omfattningen av de intrång i enskildas integritet som har tillåtits genom lagstiftning.

Sammantaget ansåg regeringen[8], i likhet med både Integritetsskyddskommittén och Grundlagsutredningen, att det fanns ett behov av att stärka skyddet för den personliga integriteten i grundlag. En reglering som ger ett stärkt integritetsskydd borde därför införas i regeringsformen.

I likhet med Integritetsskyddskommittén ansåg regeringen att den nya grundlagsbestämmelsen inte skulle utformas som en absolut rättighet i den meningen att den endast skulle kunna inskränkas genom ändring i grundlag. I stället borde det utvidgade integritetsskyddet kunna inskränkas i enlighet med bestämmelserna i 2 kap. 12 § RF (som i dag motsvaras av 2 kap. 20 och 21 §§ RF). Det skulle innebära – med några få undantag – att inskränkningar i integritetsskyddet bara skulle kunna göras i lag. Det skulle också ställas krav på att begränsningarna ska vara nödvändiga för att tillgodose ett ändamål som är godtagbart i ett demokratiskt samhälle. Begränsningarna skulle inte få gå utöver vad som är nödvändigt med hänsyn till de ändamål som har föranlett begränsningarna och inte heller sträcka sig så långt att de skulle utgöra ett hot mot den fria åsiktsbildningen. Som Integritetsskyddskommittén hade påpekat var en följd av denna reglering bl.a. att lagstiftaren tvingas att tydligt redovisa vilka avvägningar som gjorts vid proportionalitetsbedömningen. Detta kunde förväntas öka förutsättningarna för att avvägningarna i fråga om integritetsintrånget blev mer ingående belysta och att de presenterades på ett sådant sätt att kvaliteten i lagstiftningen skulle höjas ytterligare.[9]

[7] Prop. 2009/10:80 s. 175.
[8] Prop. 2009/10:80 s. 176.
[9] Prop. 2009/10:80 s. 176 ff.

Genom att lyfta upp centrala inslag i integritetsskyddet på grundlagsnivå betonar lagstiftaren respekten för människovärdet och för varje människas rätt till självbestämmande. Om skyddet för den personliga integriteten däremot ges en svag förankring i grundlagen, kan följden bli att tillräcklig vikt inte läggs vid integritetsskyddsaspekterna när ny lagstiftning arbetas fram. De negativa konsekvenserna av en sådan underlåtenhet från grundlagsstiftarens sida kan sägas ha blivit synliggjorda genom Integritetsskyddskommitténs analys.[10]

16.1.2 Hur lagstiftningsarbetet ska gå till

Integritetsskyddskommitténs förslag ledde sedan till att det i 2 kap. 6 § andra stycket RF infördes en bestämmelse som anger att var och en, utöver vad som i övrigt gäller enligt paragrafen, gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, som görs utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

Denna grundlagsändring innebar en väsentlig förstärkning av integritetsskyddet och påverkar därmed lagstiftningsarbetet genom att

- fler tänkbara intrång från det allmännas sida än enbart lagstiftning omfattas av grundlagens principiella förbud,
- intrång av visst slag i rätten till skydd för den personliga integriteten endast får tillåtas i form av lag,
- begränsningar endast får göras för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle,
- sådana tillåtande lagregler bara får införas om begränsningen i rätten till skydd för den personliga integriteten inte går utöver vad som är nödvändigt med hänsyn till det ändamål som föranlett den,
- begränsningen inte heller får sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar, och
- begränsningen inte får göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning.

[10] SOU 2008:3 s. 15.

Det utvidgade grundlagsskyddet medför att intrång i rätten till skydd för den personliga integriteten måste föregås av en sådan proportionalitetsbedömning som avses i 2 kap. 20 och 21 §§ RF. Visserligen medför redan Europakonventionen att alla inskränkningar i den personliga integriteten måste stå i rimlig proportion till det syfte som ska tillgodoses genom intrånget. Genom att tillåtligheten av inskränkningarna kopplas till kraven i 2 kap. 20 och 21 §§ RF tvingas emellertid lagstiftaren att redovisa sina bedömningar i proportionalitetsfrågan, bland annat för att minska risken för att inskränkningarna underkänns såsom grundlagsstridiga vid en prövning enligt 11 kap. 14 § RF.

När proportionalitetsbedömningen på så sätt kommer i blickpunkten ges också möjlighet till offentlig debatt och ytterligare analys under lagstiftningsprocessen och inte minst under riksdagens behandling av förslaget till lag.[11]

16.2 Integritetskommitténs uppföljning

16.2.1 Urval och metod

Integritetskommitténs uppdrag har varit att följa upp och analysera effekterna i *lagstiftningsarbetet* av det förstärkta grundlagsskyddet. Detta har vi gjort genom att granska betänkanden från åren 2011–2016 i vilka lagstiftningsåtgärder har övervägts. Därefter har kommittén även granskat hur lagstiftningsarbetet fortsatt i eventuella propositioner. Däremot har vi inte granskat arbete med regleringar i andra former, som förordningar eller myndighetsföreskrifter.

Kommittén har inriktat sin uppföljning och analys på frågan om vilket genomslag bestämmelsen i RF 2:6 andra stycket har fått i lagstiftningsarbetet.

Vårt tillvägagagångssätt har varit att granska alla remissyttranden från Datainspektionen, Justitiekanslern, Justitieombudsmannen, Lagrådet och Advokatsamfundet i vilka bestämmelsen i RF 2:6 andra stycket berörs. Därefter har undersökts om regeringen gått vidare med en proposition och i så fall i vad mån bestämmelsen i RF 2:6 andra stycket har berörts.

[11] SOU 2008:3 s. 189.

Utöver uppdraget till Integritetskommittén att följa upp lagstiftningsarbetet, har regeringen såvitt vi känner till inte vidtagit några andra uppföljande åtgärder med anledning av RF 2:6 andra stycket. En sådan åtgärd skulle exempelvis kunna vara att undersöka om förordningar, myndighetsföreskrifter eller myndigheternas faktiska handlande är förenliga med bestämmelsen i RF 2:6 andra stycket.

16.2.2 Resultatet av granskningen

Under perioden 2011–2016 har Datainspektionen avgivit sammanlagt 452 yttranden över olika lagförslag. RF 2:6 andra stycket nämns i 46 av dessa yttranden, dvs. i cirka 10 procent av alla yttranden.

En återkommande synpunkt i dessa yttranden från Datainspektionen är att integritetsanalysen eller proportionalitetsbedömningen är bristfällig eller helt saknas. Några exempel på detta:

- I yttrandet över betänkandet *Särskilda spaningsmetoder*[12] anför Datainspektionen att ”det förstärkta integritetsskyddet i 2 kap. 6 § andra stycket regeringsformen innebär också att lagstiftaren tydligt måste redovisa vilka avvägningar som gjorts vid proportionalitetsbedömningen. Någon sådan redogörelse har utredningen inte lämnat”.[13] I den efterföljande propositionen saknas fortfarande en mer utförlig redogörelse än betänkandet när det gäller vilka avvägningar som gjorts vid proportionalitetsbedömningen.[14]
- I yttrandet över en departementspromemoria om kustbevakningsdatalag anför Datainspektionen att proportionalitetsbedömningen enligt RF 2:6 andra stycket – mellan Kustbevakningens behov av personuppgiftsbehandling i sin verksamhet å ena sidan och den enskildes rätt till skydd för intrång i den personliga integriteten å andra sidan – behöver göras tydligare. ”Datainspektionen anser att det fortsatta lagstiftningsärendet bör innehålla en djupare analys och diskussion om de proportionalitetsavvägningar som har gjorts”.[15] Den efterföljande propositionen innehåller – med ut-

[12] Polismetodutredningens betänkande *Särskilda spaningsmetoder* (SOU 2010:103).
[13] Datainspektionens yttrande den 20 juni 2011 med dnr 445-2011.
[14] Prop. 2011/12:55 *De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation*.
[15] Datainspektionens yttrande den 29 augusti 2011 med dnr 679-2011.

trycklig hänvisning till Datainspektionens remisssvar – en mer omfattande redogörelse än betänkandet när det gäller avvägningen mellan Kustbevakningens behov av att behandla personuppgifter och skyddet för den personliga integriteten.[16]

- I yttrandet över en promemoria med utkast till lagrådsremiss avseende register för viss forskning, anför Datainspektionen att ”de frågor som ska regleras med förslaget är förtjänta av en grundligare utredning än den som presenteras i promemorian med utkast till lagrådsremiss Med största sannolikhet skulle en djupare analys av frågorna på längre sikt innebära vinster såväl för forskningens trovärdighet och möjligheter som för deltagarnas personliga integritet”.[17] Den resulterande lagstiftningen gavs tidsbegränsad giltighet. Regeringen beslutade i januari 2013 att tillkalla en särskild utredare med uppdrag att närmare utreda förutsättningarna för registerbaserad forskning, varvid hänsyn skulle tas till bland annat skyddet för den enskildes integritet.[18]

En annan återkommande synpunkt från Datainspektionen är att myndigheten anför att bestämmelsen i RF 2:6 andra stycket kan vara eller är tillämplig. Detta framförs utan att Datainspektionen fördjupar sig i frågan om i vad mån förslaget är förenligt med bestämmelsen, eller närmare går in på vad bestämmelsen innebär för det aktuella förslaget. Några exempel på detta:

- I yttrandet över betänkandet *En ny biobankslag*[19], förutsätter Datainspektionen att ”eventuella författningsförslag kommer att föregås av noggranna överväganden och analyser av integritetsaspekter som gör sig gällande för tidigare och kommande provgivare”.[20] Förslaget har inte förts vidare till en proposition.
- I yttrandet över promemorian *Hälsoväxling för aktivare rehabilitering och omställning på arbetsplatserna* anför Datainspektionen att ”det föreslagna informationsutbytet kan även innebära en så betydande kartläggning av enskildas personliga förhållanden att

[16] Prop. 2011/12:45 *Kustbevakningsdatalag*, se bland annat s. 66 ff.
[17] Datainspektionens yttrande den 15 februari 2013 med dnr 156-2013.
[18] Registerforskningsutredningens betänkandet *Unik kunskap genom registerforskning* (SOU 2014:45).
[19] Biobanksutredningens betänkande *En ny biobankslag* (SOU 2010:81).
[20] Datainspektionens yttrande den 1 april 2011 med dnr 1939–2010.

2 kap. 6 § andra stycket regeringsformen blir tillämplig. I ett konkret lagstiftningsärende innebär det att det intrång som sker i den enskildes personliga integritet måste vara befogat och inte större än nödvändigt. Intrånget ska mötas av integritetshöjande bestämmelser till förmån för den enskilde vars personuppgifter behandlas".[21] Datainspektionen utvecklar inte i yttrandet vad det får för konsekvenser om bestämmelsen skulle vara tillämplig. I den efterföljande lagrådsremissen redovisar regeringen utförligt sina överväganden i integritetsfrågan, utan att uttryckligen hänvisa till RF 2:6 andra stycket.[22]

I ett remissvar fick Datainspektionen anledning att diskutera den närmare innebörden i RF 2:6 andra stycket:

- I yttrandet över betänkandet *Myndighetsdatalag*[23] anför Datainspektionen att "det resonemang som ligger till grund för utredningens ställningstagande utmynnar i bedömningen att bestämmelsen i 2 kap. 6 § andra stycket regeringsformen inte syftar till att ange vilka bestämmelser om exempelvis behandling av personuppgifter som ska ha form av lag i stället för förordning. Enligt utredningen har bestämmelsen i stället primärt funktionen att bland sådana intrång som omfattas av lagkravet i 8 kap. 2 § första stycket regeringsformen skilja ut de intrång som är så kvalificerade att de ska omfattas av de särskilda begränsningar som enligt 2 kap. 20–22 §§ gäller för riksdagens möjligheter att besluta om en rättighetsinskränkande lag". I sitt yttrande tar Datainspektionen tydligt avstånd från betänkandets tolkning av RF 2:6 andra stycket. Enligt Datainspektionen "råder det inga tvivel om att bestämmelsen i 2 kap. 6 § andra stycket regeringsformen utgör en från 8 kap. regeringsformen fristående bestämmelse, som ställer krav på lagform".[24] Betänkandet har inte lett till lagstiftning.

Vi har även granskat yttranden från Advokatsamfundet och Justitiekanslern och följt upp hur deras synpunkter tagits omhand i det eventuella, fortsatta lagstiftningsarbetet. Advokatsamfundet och

[21] Datainspektionens yttrande den 3 juni 2016 med dnr 662-2016.
[22] Lagrådsremiss den 7 juli 2016, *Hälsoväxling för aktivare rehabilitering och omställning på arbetsplatserna*.
[23] Informationshanteringsutredningens betänkande *Myndighetsdatalag*, (SOU 2015:39).
[24] Datainspektionens yttrande den 20 november 2015 med dnr 1125-2015.

Justitiekanslern har under perioden 2011–2016 relativt ofta framfört synpunkter på hur integritetsaspekter tagits omhand i betänkanden.

Advokatsamfundet efterlyser ofta bättre redovisningar av ett förslags integritetsaspekter – detta har samfundet gjort i sammanlagt 30 yttranden över lagförslag under den aktuella perioden. Vanligtvis görs detta utan uttrycklig hänvisning till RF 2:6 andra stycket, men i enstaka yttranden hänvisar samfundet uttryckligen till bestämmelsen.

Några exempel på synpunkter från Advokatsamfundet:

- I yttrandet över promemorian *Förslag till vissa ändringar av förslagen i departementspromemorian Informationsutbyte vid samverkan mot grov organiserad brottslighet*[25] konstaterar Advokatsamfundet – utan att uttryckligen nämna RF 2:6 andra stycket – att det ”saknas nödvändig analys och bedömning av hur informationsflödet mellan myndigheterna påverkar den personliga integriteten och rättssäkerheten för individen, liksom att det saknas en erforderlig proportionalitetsbedömning i fråga om avvägningen mellan hänsynen till den enskildes integritet och rättssäkerhet å ena sidan och myndigheternas behov av uppgifter för sin brottsbekämpande verksamhet å den andra”.[26] I den efterföljande propositionen ägnar regeringen ett särskilt kapitel åt att redovisa sina överväganden beträffande ”balans mellan effektivitet och integritet”. Regeringsformens 2 kap. nämns i propositionen, utan att regeringen särskilt går in på 2 kap. 6 § andra stycket. Regeringen anser sammanfattningsvis att ”förslaget kan få konsekvenser för den personliga integriteten och att dessa konsekvenser, i motsats till vad Sveriges advokatsamfund anser, är tillräckligt belysta”.[27]
- I yttrandet över promemorian *Polisens tillgång till signalspaning i försvarsunderrättelseverksamhet*[28] uppger Advokatsamfundet – utan att uttryckligen nämna RF 2:6 andra stycket – att samfundet, på det presenterade underlaget, inte är ”berett att tillstyrka att även RKP [Rikskriminalpolisen] får inrikta signalspaning i försvarsunderrättelseverksamhet. För att det över huvud taget ska vara möjligt att överväga att utvidga den krets som ska kunna inrikta

[25] Ds 2014:30.
[26] Advokatsamfundets yttrande den 25 november 2015 med beteckningen R-2015/2121.
[27] Prop. 2015/16:167 *Informationsutbyte vid samverkan mot organiserad brottslighet*, s. 46.
[28] Ds 2011:44.

signalspaning, krävs en ingående analys av behovet för att kunna ta ställning till om detta kan anses godtagbart, med hänsyn till rättssäkerhets- och integritetsskyddsintressen".[29] Även lagrådet ansåg att promemorian och lagrådsremissen gav begränsad vägledning när det gällde proportionaliteten, eller "nödvändigheten med hänsyn till ändamålet, av de begränsningar i skyddet enligt 2 kap. 6 § regeringsformen som förslaget skulle kunna innebära".[30] Den efterföljande propositionen innehåller i allt väsentligt samma behovsanalys som promemorian.[31] Propositionen ger inte heller mer hjälp för proportionalitetsbedömningen än promemorian.

16.3 Integritetskommitténs slutsatser

Det är enligt kommitténs uppfattning svårt att med någon säkerhet uttala sig om hur lagstiftningsarbetet skulle ha bedrivits om inte RF 2:6 andra stycket hade tillkommit den 1 januari 2011. Även före 2011 gällde enligt somliga förarbetsuttalanden och Datainspektionen, att viss hantering av personuppgifter krävde lagform – med därtill hörande noggranna överväganden om behovet.[32] En jämförelse med tiden före den 1 januari 2011 försvåras också av att förutsättningarna för lagstiftningsarbetet har förändrats i takt med att nya arbetssätt och ny teknik utvecklats och börjat användas inom den offentliga förvaltningen.

Det som går att uttala sig om, är om och i så fall hur RF 2:6 andra stycket används och kommer till uttryck i lagstiftningsarbetet. På denna punkt visar vår uppföljning av lagförslag som i remisshanteringen fått kritik med avseende på RF 2:6 andra stycket, att bestämmelsen åberopas och används, fast på mycket skiftande sätt. Bestämmelsen kan således sägas ha haft effekt genom att den eller de krav som ställs i bestämmelsen nämns och tillämpas. Det görs, om än i varierande omfattning, i flera led i lagstiftningskedjan: i betänkanden, remissyttranden och i propositioner.

Vi kan samtidigt konstatera att det inte är ovanligt att remissinstanser, särskilt Datainspektionen, anser att utredningar har allvar-

[29] Advokatsamfundets yttrande den 8 mars 2012 med beteckningen R-2011/1790.
[30] Prop. 2011/12:179 *Polisens tillgång till signalspaning i försvarsunderrättelseverksamhet*, s. 31.
[31] Prop. 2011/12:179 *Polisens tillgång till signalspaning i försvarsunderrättelseverksamhet*.
[32] Prop. 1997/98:44 s. 41 där det hänvisas till äldre förarbetsuttalanden.

liga brister med avseende på hur utredningarna har tillämpat kraven i RF 2:6 när det gäller att redovisa förslagens konsekvenser för den personliga integriteten och när det gäller att redovisa sin bedömning av förslagens proportionalitet.

Av vår granskning framgår även att regeringen ibland reparerar bristerna eller tar ställning till – åtminstone vissa delar av – den kritik som riktats mot utredningar med avseende på den aktuella bestämmelsen i regeringsformen. Detta görs dock inte i alla lagstiftningsärenden där regeringen går vidare med en proposition. Det är också många utredningar som inte lett till fortsatta lagstiftningsåtgärder. Skälen till detta kan vara svåra att med någon säkerhet uttala sig om. Det kan inte uteslutas att avstannandet av lagstiftningsarbetet i vissa fall delvis beror på kritik som i remissförfarandet framförts med avseende på RF 2:6 andra stycket. Eftersom det är så många betänkanden som inte har lett till lagstiftning, anser kommittén att det inte går att dra några säkra slutsatser beträffande Regeringskansliets beredning av lagstiftningsärenden där RF 2:6 andra stycket är av betydelse.

Även i de fall regeringen i någon mån reparerar bristerna i det underliggande betänkandet, görs detta först i skedet efter remissbehandlingen. Det betyder att remissinstanserna inte har kunnat ta del av den mer utförliga redogörelsen för förslagets integritetsaspekter. Det innebär i sin tur en risk för att en del viktiga synpunkter från remissinstanserna avseende integritetsfrågan inte kommer fram under remisshanteringen. Riksdagen får dock ta del av regeringens eventuella förbättringar av redogörelserna för integritetsaspekterna, vilket i sig är av stor betydelse för integritetsskyddet och uppfyller ett väsentligt syfte med det förstärkta grundlagsskyddet.

Sammantaget anser Integritetskommittén att det är otillfredsställande att bestämmelsen i RF 2:6 andra stycket tillämpas på så olika sätt av utredningar, myndigheter och inom Regeringskansliet. Det finns olikheter både avseende *när* bestämmelsen överhuvudtaget anses vara tillämplig och i så fall *hur* den ska tillämpas. Det saknas uppenbarligen en enhetlig förståelse av bestämmelsens närmare innebörd och hur den ska tillämpas. Särskilt tydligt framgår detta av de olika tolkningar av bestämmelsen som framförts i betänkandet *Myndighetsdatalag* respektive i Datainspektionens yttrande över betänkandet.

En mer enhetlig förståelse och tillämpning av bestämmelsen skulle enligt vår bedömning gynna såväl integritetsskyddet som digitali-

seringen av förvaltningen, genom att det tydligare skulle framgå vilka avvägningar som ett förslag aktualiserar. Lagstiftningsarbetet skulle inte på samma sätt som i dag riskera att tappa tempo på grund av att beredningsunderlag behöver kompletteras relativt sent i lagstiftningsprocessen – vilket ibland överhuvudtaget inte låter sig göras. En mer enhetlig förståelse och tillämpning av bestämmelsen skulle också spara resurser för den sammanlagda arbetsinsatsen i lagstiftningsprocessen. Utifrån dessa bedömningar lämnar kommittén de förslag som följer nedan.

16.4 Förslag till åtgärder

16.4.1 Ändring i kommittéförordningen

Integritetskommitténs förslag: Regeringen bör i kommittéförordningen (1998:1474) införa en bestämmelse som föreskriver att om förslagen i ett betänkande har betydelse för den personliga integriteten i de fall som avses i 2 kap. 6 § andra stycket regeringsformen, ska konsekvenserna i det avseendet anges i betänkandet.

Kommittén anser att det är angeläget att statliga kommittéer och särskilda utredare blir bättre på att uppmärksamma och tillämpa det grundlagsfästa kravet på lagstiftningsarbetet som stadgas i RF 2:6 andra stycket.

Kommittéförordningen är en reglering som på ett konkret och nära sätt styr arbetet i statliga utredningar (kommittéer och särskilda utredare). Vi noterar att kommittéförordningen saknar krav på konsekvensanalyser av förslag i förhållande till RF 2:6 andra stycket och till den personliga integriteten överhuvudtaget.

Det finns inget hinder mot att i kommittéförordningen påminna om rättigheter för enskilda eller skyldigheter för det allmänna som framgår av regeringsformen. Tvärtom kan sägas att detta är en inte oväsentlig del av innehållet i kommittéförordningen. Exempelvis föreskriver kommittéförordningen en skyldighet för utredningar att redovisa konsekvenser för jämställdheten mellan kvinnor och män, samtidigt som det i 2 kap. 13 § RF stadgas att lag eller annan före-

skrift inte får innebära att någon missgynnas på grund av sitt kön, jämställdhet och motsvarande.

Kommittén anser att kommittéförordningen på motsvarande sätt som för jämställdheten, bör innehålla en påminnelse om vad 2 kap. 6 § andra stycket RF innebär för utredningsarbetet. Vi anser därför att regeringen bör införa en bestämmelse i kommittéförordningen med innebörden att om ett förslag har betydelse för den personliga integriteten i de fall som avses i 2 kap. 6 § andra stycket RF (dvs. när det är frågan om ett sådant intrång som avses i bestämmelsen), så ska konsekvenserna i det avseendet anges i betänkandet.

16.4.2 Vägledning från Regeringskansliet om konsekvensbedömningar

Integritetskommitténs bedömning: Regeringskansliet bör utvärdera, utveckla och vid behov uppdatera den av Datainspektionen utgivna vägledningen för integritetsanalys.

De framkomna brister som är aktuella här, har enligt kommitténs uppfattning ofta sin grund i att bestämmelsen i RF 2:6 andra stycket är svårtillämpad och att bestämmelsens förarbeten är relativt allmänt hållna.

Den kritik som framförs i remissförfarandet är många gånger specifikt inriktad på det aktuella förslaget, och ger därmed sällan närmare vägledning för hur regeringen eller framtida utredningar ska förhålla sig för att undvika liknande brister i kommande utredningar.

Datainspektionen har givit ut en vägledning för integritetsanalyser. Syftet med vägledningen är att underlätta arbetet med att analysera konsekvenserna för den personliga integriteten vid personuppgiftsbehandling när förslag till nya lagar och andra föreskrifter tas fram. Datainspektionen förklarar behovet av denna vägledning med att myndigheten ”i remissyttranden över lagförslag många gånger tvingas konstatera att underlaget i betänkanden inte är tillräckligt utförligt för att inspektionen ska kunna ta ställning till integritetsriskerna med lagförslagen.”[33]

[33] Datainspektionens *Vägledning för integritetsanalys* (september 2016).

Utifrån sin uppföljning av lagstiftningsarbetet, instämmer kommittén i Datainspektionens bedömning av behovet av en sådan vägledning. Enligt vår uppfattning ligger ansvaret för att till kommittéer och särskilda utredare tillhandahålla vägledning av detta slag, närmast på Regeringskansliet. Här kan jämföras med 33 § kommittéförordningen enligt vilken Regeringskansliet ska besluta de ytterligare föreskrifter som behövs för kommittéväsendets organisation och formerna för kommittéernas verksamhet.

Vi anser därför att Regeringskansliet bör ta över förvaltningen av nämnda vägledning för integritetsanalys. Det innebär att Regeringskansliet bör utvärdera, utveckla och vid behov uppdatera vägledningen.

Detta kan jämföras med att Regeringskansliet tagit fram olika vägledningar för att uppnå jämställdhetsintegrering i lagstiftningsprocessen.[34]

[34] Vägledningarna grundas i detta hänseende på bland annat protokoll II:14 vid regeringssammanträde den 22 juni 2016, med dnr S2016/01917/JÄM och S2016/04472/JÄM.

17 Konsekvenser av våra förslag

17.1 Inledning

I detta kapitel redogör vi för olika konsekvenser av Integritetskommitténs förslag. I avsnitt 17.2–17.12 är konsekvensbeskrivningen uppdelad efter de olika samhällsområden och företeelser som vi har behandlat i vårt delbetänkande.

Avsnitt 17.13 handlar om generella samhällsekonomiska konsekvenser av ett ökat integritetsskydd.

Avsnitt 17.14 behandlar kostnader och finansiering ur ett generellt perspektiv.

I avsnitt 17.15–17.20 går vi igenom konsekvenserna av våra förslag vad gäller den kommunala självstyrelsen, små företag, sysselsättning och service i hela landet, brottslighet och brottsförebyggande arbete, jämställdhet och integration samt klimat och miljö.

17.2 Skolan

I detta avsnitt behandlar vi konsekvenserna av vårt förslag att ge ett uppdrag till Skolverket att initiera och stödja utarbetandet av en uppförandekod för skolor.

17.2.1 Konsekvenser för individer

Konsekvenserna för individerna inom detta område rör barn. Kommittén anser att barn är särskilt viktiga att skydda mot otillbörliga intrång i den personliga integriteten.

Förslaget om uppförandekoder syftar till att förenkla tillämpningen av reglerna om integritetsskydd. Tydlig vägledning när det gäller en korrekt hantering av personuppgifter, möjliggör informa-

tionstjänster som kan vara av stort värde för barn i skolan. Det kan exempelvis handla om digitala lärplattformar och användning av sociala medier på rätt sätt.

Förslaget om att utreda utökat sekretesskydd för uppgifter om elever i skolans it-system syftar till att skydda barn mot att uppgifter lämnas ut, som kan användas för en närgången kartläggning av deras beteende, resultat, vanor och familjeliv.

17.2.2 Samhällsekonomiska konsekvenser

En positiv samhällsekonomisk effekt av förslaget om uppförandekod för skolan är att det möjliggör effektiviseringar i skolorna, genom att uppförandekoden hjälper skolorna att bedöma vilka tjänster de ska anlita och vilka krav de ska ställa vid upphandlingar. En uppförandekod gör det också enklare för leverantörer att erbjuda och utveckla tjänster som stödjer en korrekt tillämpning av dataskyddsförordningen.

Kommitténs bedömning är att det finns ett stort behov av klargöranden vad gäller integritetsskyddsfrågor inom skolan. Förslaget kan förväntas underlätta för ansvariga befattningshavare i skolväsendet. Detta kan både innebära kostnadseffektivitet i skolorna och som indirekt effekt medföra högre kvalitet i utbildningen.

17.2.3 Kostnader och kostnadsbesparingar

Kommittén uppskattar Skolverkets resursbehov för uppdraget till en halv årsarbetskraft under två års tid, motsvarande 1 miljon kronor.

Det är kommitténs uppfattning att en uppförandekod för skolan kommer att innebära mindre arbete för skolorna i deras tillämpning av dataskyddsreglerna jämfört med den resursåtgång som skulle vara nödvändig om det saknades stöd i en uppförandekod.

Förslaget om uppförandekoder innebär även kostnader för SKL och friskolornas branschorganisationer, eftersom de kommer att arbeta med att ge uppförandekoden dess innehåll.

Implementeringen av dataskyddsförordningen kommer, särskilt initialt, att kräva betydande resurser hos skolorna. Vi bedömer att tydlig vägledning i form av en uppförandekod skulle minska de utgif-

terna som kommer att behövas för att kunna tillämpa dataskyddsförordningen på rätt sätt i skolorna och hos deras leverantörer.

Enligt Skolverkets statistik fanns det i slutet av år 2016 sammanlagt 1 313 skolenheter i gymnasieskolan och 4 847 skolenheter i grundskolan. Det stora antalet skolenheter och skolhuvudmän som finns i landet, innebär att även en mycket försiktig uppskattning av den minskade resursåtgång som uppförandekoderna skulle medföra för varje skola, sammantaget uppgår till betydande besparingar för branschen.

17.3 Arbetsliv

I detta avsnitt går vi igenom konsekvenserna av vårt förslag att ge Arbetsmiljöverket i uppdrag att initiera och stödja utarbetandet av uppförandekoder för arbetslivet.

17.3.1 Konsekvenser för individer

Förslaget om uppförandekoder inom arbetslivet syftar till att förenkla och förbättra tillämpningen av reglerna om hur uppgifter om anställda ska hanteras. Förslaget har därigenom konsekvenser för en stor del av de anställda i Sverige. Kommitténs bedömning är att uppförandekoderna kommer att stärka de individuella arbetstagarnas personliga integritet. En annan konsekvens för individerna är att tydliga regler om hanteringen av personuppgifter kan underlätta för arbetsgivarna att välja lagliga och lämpliga kontroll- och övervakningsmetoder, vilka exempelvis kan förbättra säkerheten på arbetsplatsen.

17.3.2 Samhällsekonomiska konsekvenser

Uppförandekoderna förväntas möjliggöra för arbetsgivare att använda effektiva informationssystem utan att riskera att bryta mot dataskyddsförordningen. Med hjälp av uppförandekoderna får arbetsgivare vägledning om hur reglerna bör tillämpas. Reglerna gäller alla arbetsgivare i Sverige. Kommittén bedömer att många arbetsgivare direkt eller indirekt kommer att påverkas av uppförandekoderna. Tydlig vägledning för hur personuppgifter kan hanteras på ett lagligt

och lämpligt sätt, möjliggör för såväl offentliga som privata arbetsgivare att styra och utveckla sina verksamheter med hjälp av nya informationstjänster, vilket ger positiva samhällsekonomiska effekter.

17.3.3 Kostnader och kostnadsbesparingar

Kommittén uppskattar att uppdraget till Arbetsmiljöverket kommer att kräva en halv årsarbetskraft under två års tid, vilket motsvarar cirka 1 miljon kronor.

För arbetsgivar- och arbetstagarorganisationerna uppskattas arbetsinsatsen vara större, eftersom det är dessa organisationer, främst arbetsgivarorganisationerna, som ska ge koderna deras innehåll. Vi anser att det är svårt att uppskatta kostnaderna för dessa organisationer; dels kan det behövas flera olika koder, dels kan erfarenheter och förkunskaper om integritetsskydd i arbetslivet sannolikt variera mellan olika branscher och organisationer.

Tillämpningen av dataskyddsförordningen kommer, särskilt initialt, att kräva betydande resurser hos större arbetsgivare. Vi bedömer att tydliga vägledningar skulle minska utgifterna som behövs för att kunna tillämpa dataskyddsförordningen på rätt sätt. Det gäller såväl offentliga som privata arbetsgivare.

Inom de branscher där det kommer att finnas uppförandekoder, förväntas arbetsgivarna få lägre kostnader för att följa regelverket. Besparingarna är emellertid svåra att beräkna närmare, av samma skäl som anges ovan beträffande arbetsgivarorganisationernas kostnader för medverkan i framtagandet av koder.

17.4 Hälso- och sjukvård och välfärdsteknik inom socialtjänsten

I detta avsnitt ska vi gå igenom konsekvenserna av vårt förslag att ge ett uppdrag till en myndighet att initiera och stödja uppförandekoder för hälso- och sjukvården och socialtjänsten samt förslaget om ett sekretariat till förvaltningen av dessa koder. När det gäller förslagen om att genomföra tidigare utredda lagändringar och förslag till ny lagstiftning hänvisas till konsekvensutredningarna i respektive utredningar.

17.4.1 Konsekvenser för individer

Förslag om uppförandekoder inom detta område syftar till att förenkla och förbättra tillämpningen av de bestämmelser som reglerar hur verksamheterna ska hantera uppgifter om enskilda. Korrekt behandling av personuppgifter stärker individernas tillit för de myndigheter, kommuner, landsting och företag som får förtroendet att hantera uppgifterna. På så sätt kan enskilda känna sig trygga att söka den hjälp de behöver hos dessa vårdgivare och utförare av socialtjänst.

En korrekt tillämpning med hjälp av uppförandekoder kan förhindra att personuppgifter sprids otillåtet, försvanskas eller inte finns tillgängliga när de behövs för att ge den enskilde rätt vård och omsorg.

Ett gott integritetsskydd är även en förutsättning för att utveckla nya informationstjänster på området. Sådana tjänster har en stor potential att göra patienter långt mer delaktiga i sin vård än i dag.

17.4.2 Samhällsekonomiska konsekvenser

Den viktigaste samhällsekonomiska effekten av förslaget är att uppförandekoderna förväntas höja informationssäkerheten och integritetsskyddet och därmed också patient- och brukarsäkerheten inom vården och socialtjänsten. Kommittén bedömer även att en ökad klarhet om regeltillämpningen kan underlätta utvecklandet av nya informationstjänster.

Andel äldre i befolkningen påverkar hälso- och sjukvårdssystemet genom att denna grupp ofta har stora hälso- och sjukvårdsbehov. Exempelvis har över hälften i åldersgrupen 65–74 år minst två kroniska sjukdomar. För personer över 85 år är den andelen drygt 80 procent. Prognosen för andelen personer över 80 år i befolkningen framöver visar att det pågår en stor ökning. Andelen äldre i befolkningen antas börja öka i snabb takt omkring år 2025 och vara dubbelt så stor som i dag kring 2050.[1]

Denna demografiska utveckling med växande andel äldre personer jämfört med personer i arbetsför ålder gör att effektivisering av vård och omsorg är nödvändigt. Det finns därför höga förväntningar på att använda den potential som finns när det gäller att utveckla

[1] Socialstyrelsen, Öppna jämförelser 2016.

digitaliseringen av hälso- och sjukvården och socialtjänsten. Ett välbalanserat integritetsskydd och en korrekt tillämpning av dataskyddsförordningen ökar tilliten för digitaliseringen.

17.4.3 Kostnader och kostnadsbesparingar

Hälso- och sjukvården och socialtjänsten står för en stor del av de kommunala utgifterna. Potentiella effektiviseringar har därför effekt på hela samhällsekonomin. Utöver kostnadsbesparingar vid en given nivå av tjänster kan effektiviserad hälso- och sjukvård sänka sjukfrånvaron och ytterst förbättra livskvaliten för enskilda individer. Även besparingar i form av minskat lidande och kostnader för patient- och klientskador innebär en vinst för samhället.

I rapporten Bortom IT[2] anförs beträffande användning av digitala tjänster inom hemtjänsten att det skulle kunna leda till besparingar på 12–42 miljarder kronor på nationell nivå fram till år 2020. Potentialen för digitaliseringens möjligheter inom hälso- och sjukvård är enligt denna rapport mycket stor, både vad gäller hälsa (förbättrad hälsa och/eller uteblivet lidande) och ekonomi. Författarna bedömer att ett golv för besparingarna är 3 miljarder kronor per år, en summa som kan öka i takt med att teknikutvecklingen gör det möjligt för fler enskilda att sköta en större andel av sin vård själva.

Det finns uppgifter[3] om att vid en systematisk användning av digital teknik kan vårdenhetskostnaderna minska med 25 procent över en tioårsperiod. Det skulle enligt dessa uppgifter innebära en bruttobesparing på 180 miljarder kr fram till år 2025.

En annan rapport[4] talar om att Sverige skulle kunna spara 10 miljarder kronor fram till år 2021 om telemedicin användes vid vård av äldre och långtidssjuka.

Arbetetet med att ta fram uppförandekoder för hälso- och sjukvård och socialtjänst kommer att medföra kostnader för den myndighet som ska ansvara för att initiera och stödja arbetet med uppförandekoderna. Det kommer även medföra kostnader för de per-

[2] Bortom IT. Om hälsa i en digital tid. Institutet för framtidsstudier, Forskningsrapport 2016/2, s. 67.
[3] Värdet av digital teknik i den svenska vården, McKinsey&Company, juni 2016.
[4] Accelerating sustainable growth, The economical and social impact of enhandced Information and Communications Technology in the Nordics and Baltics, Deloitte Telia Company, September 2016.

sonuppgiftsansvariga offentliga och privata vårdgivarna som ansvarar för att uppförandekoder tas fram och kanske även för deras personuppgiftsbiträden. Datainspektionen kommer vidare ha kostnader för att stödja framtagandet av koden samt för att pröva och godkänna densamma.

Med stöd av inhämtade uppgifter från Norge uppskattar vi de löpande kostnaderna för ett myndighetssekretariat till cirka 3 miljoner kronor per år, främst avseende personalkostnader.

Uppförandekoderna kommer att underlätta för verksamheterna att tillämpa tvingande bestämmelser, vilket kommer att minska den förväntade kostnaden för att anpassa verksamheterna till kommande lagstiftning för såväl offentliga som privata aktörer. Vidare bedömer kommittén att en indirekt effekt av att förbättra hanteringen av personuppgifterna genom tillämpningen av en gemensam uppförandekod är kostnadsbesparingar för vårdgivarna eftersom detta förväntas bidra till att vårdskador kan undvikas.

Förslagen kommer även att innebära vissa besparingar på sikt, på grund av att ändringar av arbetssätt och system efter hand inte kommer att behöva vidtas lika ofta, när vårdgivare och de som bedriver socialtjänst redan från början i samband med upphandling och införande, kommer att veta hur de ska gå tillväga för att uppfylla dataskyddsförordningens krav.

Uppförandekoder förväntas alltså underlätta implementering och tillämpning av gällande rätt hos de ansvariga aktörerna. Vi kan göra en översiktlig illustration av den minskade kostnadsökningen med kommunerna som exempel. Det finns 290 kommuner. Alla dessa kommer att behöva satsa resurser på att implementera dataskyddsförordningen och andra bestämmelser som har anpassats till förordningen. Utan stöd av de gemensamma uppförandekoderna skulle varje kommun uppskattningsvis och i genomsnitt behöva ha en person som arbetar deltid med att tolka bestämmelser och se till att kommunens personuppgiftshantering och informationssäkerhetsarbete uppfyller alla krav. Om i stället en stor del av tolkningarna görs gemensamt i form av ett arbete med uppförandekoder kan de förväntade kostnaderna för implementeringen bli lägre. Med ett bra tillämpningsstöd kan en kommun klara sig med betydligt mindre resurser som arbetar med dessa frågor. Det skulle minska de förväntade utgifterna betydligt. Motsvarande gäller för de minskade implementeringskostnaderna för landsting och privata vårdgivare.

Enligt uppgifter från Vårdgivarregistret finns över 18 000 vård- och omsorgsgivare i Sverige. Det skulle innebära en stor samhällsekonomisk vinst att kunna minska kostnaderna för implementeringen av dataskyddsförordningen hos alla dessa.

17.5 E-förvaltning

I detta avsnitt går vi igenom konsekvenserna av våra förslag att:

- ge ett uppdrag åt den myndighet som får det samlade ansvaret för den offentliga förvaltningens digitalisering, att inrätta ett kompetenscenter för anskaffning och användning av externa it-tjänster,
- genomföra en utredning med uppdrag att lämna förslag till tystnadsplikt för leverantörer av molntjänster och andra personuppgiftsbiträden, och
- regeringens digitala strategi för statsförvaltningen kompletteras med ett inriktningsmål om personlig integritet.

Vad gäller förslaget att myndigheten med ansvar för den offentliga sektorns digitalisering ska ges i uppdrag att värna integriteten och stödja utarbetande av uppförandekoder – föreslås detta redan i betänkandet *digitalforvaltning.nu*[5]. När det gäller konsekvenserna av detta förslag hänvisar vi till nämnda betänkande.

17.5.1 Konsekvenser för individer

Kommitténs båda förslag att inrätta ett kompetenscenter och att regeringens digitala strategi kompletteras med inriktningsmål om personlig integritet, syftar till att stärka den personliga integriteten i e-förvaltningens hantering av personuppgifter. Det kommer att få direkta konsekvenser för de individer vilkas uppgifter hanteras inom den offentliga förvaltningen.

[5] Utredningens om effektiv styrning av nationella digitala tjänster delbetänkande *digitalforvaltning.nu* (SOU 2017:23)

Ett ökat integritetsskydd handlar bland annat om minskad risk för att personuppgifter sprids otillåtet, förvanskas eller hanteras på andra otillbörliga sätt inom e-förvaltningen.

17.5.2 Samhällsekonomiska konsekvenser

Våra förslag syftar till att ta tillvara fördelarna med digitaliseringen genom att möjliggöra en laglig och korrekt personuppgiftshantering i utvecklingen av offentlig sektor. Individernas tillit för e-tjänster möjliggör digitalisering vilket i sig möjliggör en betydande effektivisering inom staten, kommuner och landsting och för enskilda individer och företag i kontakter med dessa. Sammantaget bedömer kommittén att de positiva samhällsekonomiska effekterna är stora, när man tar hänsyn till dessa indirekta effekter av förslagen.

Vad gäller förslaget om tystnadsplikt innebär det en möjlighet för offentlig sektor att alls kunna använda molntjänster och outsourcing för uppgifter som omfattas av sekretess. Tystnadsplikten möjliggör därför betydande effektivisering i offentlig sektor.

17.5.3 Kostnader och kostnadsbesparingar

Kommittén uppskattar att uppdraget att inrätta ett kompetenscenter för frågor som rör anskaffning och användning av externa it-tjänster, kommer att kräva en årsarbetskraft för den myndighet som får det samlade ansvaret för den offentliga förvaltningens digitalisering. Resursåtgången motsvarar en årlig kostnad om ungefär 1 miljon kronor.

Förslaget att inrätta ett kompetenscenter kan komma att underlätta upphandlingar och medföra att de genomförs på ett mer effektivt sätt, exempelvis genom att rätt krav ställs och att ändamålsenliga tjänster därmed upphandlas. Ett kompetenscenter kan således minska det allmännas utgifter och bidra till att medlen används mer effektivt.

17.6 Konsumentområdet

I detta avsnitt går vi igenom konsekvenserna av vårt förslag att ge Konsumentverket i uppdrag att initiera och stödja utarbetandet av uppförandekoder för branscher med kommersiella ändamål. Vi behandlar också konsekvenserna av vårt förslag om att ge Konsumentverket i uppdrag ett förstärka sin tillsyn.

17.6.1 Konsekvenser för individer

Kommitténs förslag syftar till att stärka möjligheten för individen att ta ställning till och bestämma över hur de egna personuppgifterna används. Förslagen kan bidra till att skapa förutsättningar för konsumenterna att fatta mer välgrundade köpbeslut utifrån kunskaper om hur deras personuppgifter hanteras.

Förslaget om uppförandekoder kan ha särskilda konsekvenser för barn. Uppförandekoderna skulle nämligen kunna innehålla vägledning för hur samtycke kan inhämtas från vårdnadshavare när detta krävs. Om en sådan vägledning blir verklighet, medför det ett bättre skydd för unga, eftersom de inte hamnar i situationer där deras personuppgifter hanteras utan laglig grund. Motsvarande gäller för personer med nedsatt beslutsförmåga.

17.6.2 Samhällsekonomiska konsekvenser

Förslagen påverkar alla företag som hanterar konsumenters personuppgifter digitalt. Ett välfungerande integritetsskydd inom området kan stärka konsumenten och förbättra marknadens funktionssätt. Privatkonsumtionen utgör en betydande del av samhällsekonomin. Vidare påverkar integritetsskyddet konsumenternas förtroende för och användning av bland annat medietjänster och elektroniska betaltjänster, vilka i sig har samhällsekonomiska effekter.

Kommittén bedömer att förslagen även kommer underlätta dataportabilitet för alla tjänster som har stort beroende av personuppgifter, till exempel sociala medier. Dataportabilitet bedöms bidra till ökad konkurrens och därmed samhällsekonomisk effektivitet.

17.6.3 Kostnader och kostnadsbesparingar

Kommittén uppskattar kostnaderna för Konsumentverket att initiera och stödja utarbetandet av uppförandekoder till cirka en halv årsarbetskraft under två års tid, vilket motsvarar ungefär 1 miljon kronor.

För branschorganisationerna uppskattas arbetsinsatsen vara större, eftersom det är dessa organisationer som ska ge koderna deras innehåll. Vi bedömer att det är svårt att uppskatta kostnaderna för dessa organisationer, eftersom det kan behövas olika koder för olika branscher. Erfarenheter och förkunskaper om integritetsskydd varierar dessutom mellan olika branscher och organisationer.

Även om den samlade resursåtgången för branschorganisationerna skulle uppgå till flera gånger mer än Konsumentverkets resursbehov för denna uppgift, bör denna utgift ställas i relation till storleken på de möjliga kostnadsminskningarna som uppförandekoder kan bidra till inom detta område. Implementeringen av dataskyddsförordningen kommer, särskilt initialt, att kräva betydande resurser hos företagen. Vi bedömer att tydliga vägledningar skulle minska utgifterna som behövs för att kunna tillämpa dataskyddsförordningen på rätt sätt hos företagen.

Kostnadsminskningarna skulle kunna illustreras med följande räkneexempel. En årlig minskad resursåtgång hos 1 000 företag, om i genomsnitt en dags arbete för en kvalificerad anställd per företag, skulle uppskattningsvis kunna innebära en årlig besparing om sammanlagt cirka 4 miljoner kronor för de 1 000 företagen.

17.7 Försäkringsverksamhet

Inom detta område har kommittén förslagit att det bör införas en lagregel om tystnadsplikt i försäkringsverksamhet. Det finns redan lagförslag om tystnadsplikten som kan beredas av Regeringskansliet. Vi hänvisar därför till de konsekvensbedömningar som gjorts i befintliga utredningar.

17.8 Åtgärder inom några andra områden med allvarliga eller påtagliga risker

Inom detta område har vi lämnat följande förslag:

- Regeringen bör utreda hur en säker ordning för utfärdande av fysiska legitimationer ska se ut och hur statens ansvar för den ska vara utformad.
- Regeringen bör utreda en författningsreglerad rättighet för fysiska personer att vända sig till den som ger ut en kreditupplysningspublikation för att få uppgifter om sig själv strukna innan uppgifterna publiceras.
- Det är angeläget att regeringen lämnar förslag på reglering som ger integritetsskydd vid utlämnande av kreditupplysning, oavsett hur kreditupplysningen lämnas ut. Detta kan göras med utgångspunkt i förslag som redan föreligger.
- Regeringen bör utreda en lagreglering av sådana integritetskänsliga spaningsmetoder som i dag inte är reglerade eller har svag reglering.

Det finns redan förslag om integritetsskydd vid utlämnande av kreditupplysning som behandlas av Regeringskansliet. Vi hänvisar därför till de konsekvensbedömningar som redan gjorts i befintliga utredningar. Övriga förslag som vi lagt inom detta område måste utredas vidare.

17.9 Informationssäkerhet

I detta avsnitt behandlas konsekvenserna av vårt förslag att uppdra åt MSB att följa upp vilka åtgärder myndigheter vidtar för att följa kraven i MSB:s föreskrifter (MSBFS 2016:1) om statliga myndigheters informationssäkerhet.

Det finns redan förslag om tillsynsmandat för MSB och om ett uppdrag för myndigheten avseende en nationell styrmodell, som kan

beredas av Regeringskansliet. Vi hänvisar därför till de konsekvensbedömningar som redan gjorts i befintliga utredningar.[6]

17.9.1 Konsekvenser för individer

En del myndigheter hanterar många uppgifter eller integritetskänsliga uppgifter om enskilda. Det är naturligtvis av stor betydelse för de enskildas integritetsskydd att dessa myndigheter har ett välfungerande informationssäkerhetsarbete som uppfyller kraven i MSB:s föreskrift.

17.9.2 Samhällsekonomiska konsekvenser

Ett bra informationssäkerhetsarbete hos myndigheterna kan höja medborgarnas och företagens förtroende för statens digitala tjänster, vilket kan resultera i att fler ansluter sig till sådana tjänster. En sådan effektivisering kan på sikt leda till minskade kostnader för den statliga förvaltningen.

17.9.3 Kostnader och kostnadsbesparingar

Vi bedömer att uppföljningsuppdraget kommer att kräva resurser hos MSB som sammantaget motsvarar ca en årsarbetskraft, det vill säga ungefär 1 miljon kronor som ett engångsbelopp.

17.10 Samhällets skyddsmekanismer

I detta avsnitt behandlas konsekvenserna av vårt förslag om att regeringen bör låta utreda hur en folkbildningsinsats ska organiseras och utformas samt förslaget om att Datainspektionen ska rapportera till regeringen ifall rättsmedlen är effektiva.

[6] NISU 2014 betänkande *Informations- och cybersäkerhet i Sverige* (SOU 2015:23).

17.10.1 Konsekvenser för individer

Om rättsmedlen används effektivt till skydd för enskilda ökar tryggheten för enskilda individer. Det är därför en viktig uppgift för Datainspektionens bevaka detta och hålla regeringen informerad.

Regeringen har formulerat målsättningen att Sverige ska vara bäst i världen på att utnyttja digitaliseringens möjligheter. För att nå detta mål menar vi att det krävs en omfattande och långsiktig satsning på information riktad till samtliga medborgare. Folkbildande aktiviteter kan utveckla medborgarnas medvetenhet och förståelse för digitaliseringen och dess effekter på den personliga integriteten. Insatser som riktar sig till hela befolkningen är också viktiga av demokratiska skäl. Individer i alla åldrar och från alla samhällsgrupper behöver ha tillgång till goda grundkunskaper för att kunna agera på ett säkert sätt i det digitala samhället och kunna ta tillvara sina rättigheter.

17.10.2 Samhällsekonomiska konsekvenser

Tillsynsmyndighetens uppdrag att bevaka om rättsmedlen används effektivt till skydd för enskilda och att rapportera resultatet till regeringen innebär en ökad kunskap om hur rättsmedlen fungerar i detta avseende.

Förutsättningarna för att genomföra digitaliseringen av samhället på ett demokratiskt och tillitsskapande sätt ökar om landets invånare har grundläggande kunskaper om vilka fördelar och risker som hör ihop med digitaliseringen.

17.10.3 Kostnader och kostnadsbesparingar

Kommittén föreslog redan i delbetänkandet att Datainspektionens uppdrag att följa och beskriva utvecklingen på it-området när det gäller frågor som rör personlig integritet och ny teknik, ska utvidgas till att även omfatta de legala förutsättningarna för integritetsskyddet och att myndigheten årligen ska lämna en redovisning om utvecklingen inom området till regeringen. Vi föreslog även att Datainspektionen ska få ökade resurser för detta uppdrag. Vi anser att det är naturligt att det i denna uppgift ingår att analysera om rättsmedlen är

tillräckligt effektiva för att skydda enskilda och om de uppfyller dataskyddsförordningens kvalitetskrav.

Vi anser att det är lämpligt att låta en myndighet undersöka på vilket sätt en folkbildande insats bör utformas för att ge så bra genomslag som möjligt. Vi har förutsatt att folkbildningsinsatsen bör involvera flera myndigheter och även det civila samhället. Ett uppdrag att utreda en folkbildningsinsats, bör omfatta en bedömning av kostnader och av finansieringen av insatsen.

17.11 Tillsynsmyndigheten

I detta avsnitt behandlas konsekvenserna av förslaget om att regeringen bör uppdra åt Statskontoret att göra en myndighetsanalys av Datainspektionen.

17.11.1 Konsekvenser för individer

Förslaget om en myndighetsanalys syftar ytterst till att Datainspektionens verksamhet ska vara effektiv. Myndighetens verksamhet får konsekvenser för individerna på flera sätt. Tillsynen värnar individens integritetsskydd generellt i samhället. Dessutom har Datainspektionen i uppdrag att bedriva förebyggande arbete med att informera om reglerna som ska skydda den enskildes personliga integritet. Det har därför positiva effekter för den enskilde om Datainspektionens tillsyn fungerar bra.

17.11.2 Samhällsekonomiska konsekvenser

I ett första steg är den önskade effekten av myndighetsanalysen att möjliggöra en effektiv statsförvaltning och i nästa steg att åstadkomma en välfungerande tillsyn. Tillsynen över personuppgiftshanteringen präglas av en omvärld med snabb teknikutveckling med nya aktörer och verksamheter. Det är därför nödvändigt att tillsynen är snabb och flexibel. När Datainspektionens proaktiva stöd och tillsyn fungerar väl, blir tillämpningen mer förutsägbar för företag och myndigheter, vilket också har positiva effekter på samhällsekonomin.

17.11.3 Kostnader och kostnadsbesparingar

Kommittén uppskattar Statskontorets kostnader för myndighetsanalysen till omkring 1 miljon kronor.

17.12 Forskning om personlig integritet

I detta avsnitt behandlas konsekvenserna av förslaget om att ge Vetenskapsrådet i uppdrag att fördela anslag till tvärvetenskaplig forskning avseende frågan om på vilket sätt människan påverkas av förändringar i den privata sfären och av den accelererande digitala hanteringen av personuppgifter.

17.12.1 Konsekvenser för individer

Mer kunskap från forskning kan ge regeringen, riksdagen, myndigheterna samt många företag och organisationer ett bättre kunskapsunderlag för att kunna fatta välgrundade beslut. På så sätt skapas bättre underlag för långsiktiga bedömningar när det gäller samhällets digitalisering. Välgrundade beslut i integritetsskyddsfrågor gynnar i sin tur den enskilde.

17.12.2 Samhällsekonomiska konsekvenser

Ökad kunskap bör ge bättre förutsättningar för olika satsningar på att digitalisera den offentliga förvaltningen och näringslivet. Kunskap från forskning kan generera bättre beslutsunderlag för bland annat regering och riksdag, men även för företag och myndigheter. En väl genomförd digitalisering kan leda till positiva konsekvenser för hela samhällsekonomin.

17.12.3 Kostnader och kostnadsbesparingar

Vårt förslag är att regeringen avsätter mellan 14 och 20 miljoner som ett engångsbelopp på denna slags forskning. I avsnitt 15.2.1 har vi beskrivit hur vi uppskattat detta belopp.

17.13 Generella samhällsekonomiska effekter av integritetsskydd

Behovet av offentliga åtaganden för att värna integritetsskyddet framgår av dataskyddsförordningen. EU-kommissionen redogör i sin konsekvensanalys till dataskyddsförordningen för samhällsekonomiska effekter av integritetsskyddet. Kommissionen konstaterar där att omfattningen av datadelning och datainsamling har ökat dramatiskt sedan EU:s nuvarande rättsliga ram om uppgiftsskydd antogs 1995. Teknikutvecklingen möjliggör ökad användning av personuppgifter hos både företag och myndigheter. Enskilda personer tillgängliggör själva alltmer personlig information, utan att vara medvetna om riskerna som följer av det.

Vidare uttalar kommissionen att det är avgörande för den ekonomiska utvecklingen att bygga upp förtroendet för nätmiljön. Bristande förtroende gör att konsumenterna tvekar inför e-handel och nya tjänster, inklusive e-förvaltning. Bristen på förtroende och svårtillgängliga system kommer bromsa utvecklingen av innovativ användning av ny teknik om den inte hanteras. Den kan då bli ett hinder för ekonomisk tillväxt och den offentliga sektorns möjlighet att dra fördel av en digitalisering av sina tjänster.

De tre främsta politiska målen med det nya EU-regelverket är att:

1. stärka uppgiftsskyddet med avseende på den inre marknaden, förstärka enhetlighet och förenkla lagstiftning och därigenom minska de administrativa bördorna,
2. öka effektiviteten i den grundläggande rättigheten till uppgiftsskydd och ge enskilda personer kontroll över sina rättigheter, och
3. stärka samstämmigheter i EU:s ram för uppgiftsskydd, även inom polissamarbete och inom straffrättsliga frågor.

I sin konsekvensanalys anger EU-kommissionen följande beträffande besparingar och kostnader för det nya regelverket:

> Preciseringar och förenklingar av bestämmelserna – en enda lag för hela EU och en enda kontaktpunkt för tillsyn över uppgiftsskyddet – kommer att stärka den inre marknaden bland annat genom att skillnaderna undanröjas i dataskyddsmyndigheternas administrativa formaliteter. Enbart vad gäller administrativa bördor kommer detta att göra det möjligt

sammanlagt spara ca 2,3 miljarder euro per år. (...) Kostnaderna för efterlevnaden av reglerna skulle uppgå till 320 miljoner euro per år.[7]

17.14 Generellt om kostnader och finansiering

Dataskyddsförordningen ska tillämpas. Alternativet till kommitténs förslag om uppförandekoder är således inte att myndigheter och företag avstår från att vidta åtgärder eller genomföra förändringsarbete, utan snarare att företag, myndigheter och andra organisationer tvingas lägga mer resurser på att tolka rättsläget.

Som framgått ovan, menar vi att flera av kommitténs förslag, kommer att innebära minskade kostnader för både företag och myndigheter (såväl statliga som kommunala).

Vi har lämnat förslag som innebär kostnader för det offentliga inom flera av de områden som omfattas av kommitténs analys. De kan totalt uppskattas till följande

- Skolan: 1 miljon kronor under två års tid för Skolverket.
- Arbetsliv: 1 miljon kronor under två års tid för Arbetsmiljöverket.
- Hälso- och sjukvård och välfärdsteknik inom socialtjänsten: 3 miljoner kronor årligen för E-hälsomyndigheten eller någon annan myndighet
- E-förvaltning: 1 miljon kronor årligen för den myndighet som får det samlade ansvaret för den offentliga förvaltningens digitalisering.
- Konsumentområdet: 1 miljon kronor under två års tid för Konsumentverket.
- Informationssäkerhet: 1 miljon kronor som engångsbelopp för MSB.
- Tillsynsmyndigheten: 1 miljon kronor för Statskontorets myndighetsanalys.

[7] Arbetsdokument från Kommissionens avdelningar med sammanfattning av konsekvensbedömningen som medföljer den allmänna uppgiftsskyddsförordningen, Bryssel den 25.1.2012 SEK(2012) 73 final.

- Forskning om personlig integritet: Mellan 14 och 20 miljoner kronor som ett engångsbelopp till Vetenskapsrådet.

Totalt skulle våra förslag medföra kostnader för staten på 23 till 29 miljoner kronor, varav fyra miljoner avser löpande årskostnader.

Kommittén föreslår att förslagen bör finansieras genom omfördelningar av medel från alla statliga myndigheter till de myndigheter som behöver ökade anslag för att genomföra våra förslag.

I den mån som detta inte låter sig göras, bör nödvändiga kostnader ges täckning genom att en del av överskottet i de statliga finanserna tas i anspråk.

17.15 Konsekvenser för den kommunala självstyrelsen

Förslaget om uppförandekoder innebär att kommuner och landsting kan medverka till tolkningen av regelverket och därmed kan påverka tillämpningen mer än om vad som hade varit fallet med en mer detaljerad lagstiftning. I övrigt bedömer inte kommittén att förslagen har påverkan på det kommunala självstyret.

SKL är en viktig aktör för flera av förslagen och kommer att behöva engagera sig i utarbetandet av uppförandekoder inom skolans område, hälso- och sjukvård samt socialtjänst samt övrig e-förvaltning.

17.16 Konsekvenser för små företag

Små- och medelstora företag har vanligtvis mindre tillgång till stabs- och specialistresurser samt administrativ kompetens jämfört med större företag. Det gör att krav på att anpassa sig till nya regelverk påverkar mindre företag i relativt högre utsträckning än större företag. De föreslagna uppförandekoderna syftar bland annat till att förenkla för företag att anpassa sin verksamhet till och löpande följa den nya dataskyddsförordningen. Förslagen kan därför förväntas underlätta mer för mindre än för större företag, sett i proportion till verksamhetens storlek.

Beträffande uppförandekoder bör noteras att arbetet med dessa enligt artikel 40 i dataskyddsförordningen ska ta hänsyn till bland

annat de särskilda behoven hos mikroföretag samt små och medelstora företag.

17.17 Förslagens påverkan på sysselsättning i olika regioner och för privatpersoners och företags tillgång till service

Kommittén bedömer att förslagen inte får konsekvenser för sysselsättningen i olika regioner, och inte heller för privatpersoners och företags tillgång till service.

17.18 Konsekvenser för brottsförebyggande arbete och brottslighet

Kommitténs förslag har viss påverkan på brottsförebyggande arbete och brottslighet. Nedan anges kortfattat kommitténs bedömningar.

De föreslagna uppförandekoderna förväntas göra det tydligare för anställda vad som är en korrekt och laglig hantering av personuppgifter, och vad som är att betrakta som dataintrång – vilket både kan förebygga dataintrång och underlätta brottsutredningar.

Om förslagen om uppförandekoder leder till ett välfungerande integritetsskydd, kan det öka it-säkerheten för privatpersoner och därmed sänka risken för identitetsstölder som i sin tur används för stölder, bedrägerier och liknande.

Det kan bli svårare för brottsbekämpande myndigheter att samla in data, om en uppförandekod bidrar till ökade möjligheter att välja krypterade tjänster.

Ett säkrare underlag för fysiska legitimationer skulle minska riskerna för brottslighet i form av bedrägerier och identitetsstölder.

17.19 Konsekvenser för jämställdhet och de integrationspolitiska målen

Dagens risker för den personliga integriteten får olika konsekvenser för kvinnor och män eftersom bl.a. konsumtion, arbetsmarknad och användning av sociala medier skiljer sig åt mellan kvinnor och män samt pojkar och flickor. Det är rimligt att anta att kommitténs förslag

på motsvarande sätt kommer att ge olika effekter, även om förslagen i sig är könsneutrala.

Antalet vårdtillfällen i sluten vård har legat relativt konstant under många år, cirka 1,4–1,5 miljoner vårdtillfällen per år sedan 1998. I relationen till befolkningen finns en trend mot minskat antal vårdtillfällen. Kvinnor konsumerar 54 procent av vårdtillfällena och männen 46 procent, vilket är ett förhållande som stått sig under lång tid.[8] Dessa förhållanden innebär att ökad säkerhet i vården får olika effekter på män och kvinnor.

Övervakning av arbetstagare är mer intensiv inom vissa branscher, där kvinnor utgör en större andel av de anställda än män. Detta gäller exempelvis säljare i butik, vårdbiträden samt personal i restauranger och caféer. Å andra sidan är andra, mer direkt övervakade yrken vanligare för män än kvinnor, till exempel lastbilsförare och lagerarbetare. Dessa yrken sysselsätter dock färre arbetstagare än de tidigare nämnda kvinnodominerade yrkena.

Folkbildande aktiviteter kan utjämna ojämlika förutsättningar att få del av och tillgodogöra sig nödvändiga kunskaper för att ta tillvara sina rättigheter. Det kan också göra det lättare för personer som inte har svenska som modersmål att ta tillvara sina rättigheter.

Förslaget om att utreda möjligheterna till medborgarprofilering kan i sin förlängning motverka diskriminering inom e-förvaltningen.

När det gäller sociala medier, är kvinnor generellt sett mer aktiva än män.[9] Det innebär att en förstärkning av integritetsskyddet i sociala medier kan få olika konsekvenser för kvinnor och män.

17.20 Konsekvenser för klimat och miljö

Digitaliseringen möjliggör positiva effekter för klimat och miljö genom minskade transporter eftersom fysiska möten och resor kan ersättas. Det gäller bland annat inom sjukvården, socialtjänsten, arbetslivet och konsumtion av varor och tjänster. Kommittén bedömer att förslagen kan bidra till denna utveckling genom att förenkla regeltillämpningen för personuppgiftshantering.

[8] *Effektiv vård*, SOU 2016:2, s. 92
[9] Se vårt delbetänkande, *Hur står det till med den personliga integriteten?* (SOU 2016:41), s. 375.

DEL IV

Bilagor

Kommittédirektiv 2014:65

Den personliga integriteten

Beslut vid regeringssammanträde den 8 maj 2014

Sammanfattning

En parlamentariskt sammansatt kommitté ska

- utifrån ett individperspektiv kartlägga och analysera sådana faktiska och potentiella risker för intrång i den personliga integriteten som kan uppkomma i samband med användning av informationsteknik i såväl privat som offentlig verksamhet samt inom ramen för detta arbete följa upp effekterna i lagstiftningsarbetet av förstärkningen av grundlagsskyddet för den personliga integriteten som genomfördes 2011, och
- med beaktande av samhälls- och teknikutvecklingen i stort och mot bakgrund av slutsatserna av kartläggnings- och analysuppdraget, följa upp betänkandet Skyddet för den personliga integriteten (SOU 2008:3) när det gäller behovet av att inrätta ett integritetsskyddsråd och särskilt överväga om de uppgifter som ett sådant råd i så fall bör ges lämpligen kan fullgöras av en befintlig myndighet, samt föreslå nödvändiga författningsändringar.

Kommittén får, om den bedömer att det är lämpligt, lämna ett eller flera delbetänkanden. I uppdraget ingår inte att föreslå ändringar i grundlag.

Uppdraget ska redovisas slutligt senast den 1 december 2016.

Bakgrund

Grundläggande bestämmelser om personlig integritet

Begreppet personlig integritet används i vardagligt tal vanligen för att beteckna individens värde och värdighet. Begreppet finns i både grundlag och vanlig lag, t.ex. 2 kap. 6 § andra stycket regeringsformen (RF) och 5 a § personuppgiftslagen (1998:204). Någon allmängiltig definition av begreppet har dock inte slagits fast i lagstiftningen. I ett försök att ändå beskriva vad som kan anses vara kärnan i rätten till personlig integritet har lagstiftaren uttalat att kränkningar av den personliga integriteten utgör intrång i den fredade sfär som den enskilde bör vara tillförsäkrad och där ett oönskat intrång bör kunna avvisas (prop. 2009/10:80 s. 175, prop. 2005/06:173 s. 15). I Nationalencyklopedins ordbok beskrivs den personliga integriteten som en ”rätt att få sin personliga egenart och inre sfär respekterad och att inte utsättas för personligen störande ingrepp”. Rätten till personlig integritet kan också beskrivas som en rätt att bli lämnad i fred eller en rätt till självbestämmande och valfrihet.

Grundläggande bestämmelser som har betydelse för det allmännas ansvar att skydda enskildas privatliv och integritet finns i bl.a. regeringsformen. Av målsättningsstadgandet i 1 kap. 2 § RF framgår att den offentliga makten ska utövas med respekt för den enskilda människans frihet och värdighet samt att det allmänna ska värna den enskildes privatliv och familjeliv. Vidare finns i 2 kap. 6 § RF en bestämmelse som slår fast ett skydd för förtroliga meddelanden och som även stadgar att var och en också i övrigt är skyddad gentemot det allmänna mot betydande intrång i den personliga integriteten som sker utan samtycke och innebär kartläggning eller övervakning av enskilds personliga förhållanden.

Enligt artikel 8 i den europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen), som gäller som svensk lag, har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Av 2 kap. 19 § RF följer att en lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden på grund av konventionen. En bestämmelse om respekt för privat- och familjelivet finns även i artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna. Av artikel 8 i stadgan följer vidare

bl.a. att var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

Rätten till skydd av privatlivet och den personliga integrite-ten är inte absolut. Skyddet enligt regeringsformen kan inskrän-kas genom lag (2 kap. 20 § RF). Begränsningarna får dock inte gå utöver vad som är nödvändigt med hänsyn till det ändamål som föranlett dem och inte heller sträcka sig så långt att de utgör ett hot mot den fria åsiktsbildningen. Det fordrar bl.a. att nya lagförslag, som innebär risker ur integritetssynpunkt, är väl motiverade och grundade på noggranna behovsanalyser och intresseavvägningar, att konsekvens-beskrivningarna när det gäller integritetsaspekterna är klara och begripliga samt att det är möjligt att förstå varför ett förslag valts framför ett annat, mindre ingripande, förslag för att nå ett visst efter-strävat mål (SOU 2007:22 s. 445 f.). Finns det utrymme att vidta särskilda åtgärder för att begränsa intrångets intensitet måste sådana normalt övervägas och om möjligt också vidtas. Intresset av enskil-das personliga integritet måste således vägas mot andra berättigade intressen i samhället, t.ex. yttrandefrihet, ett tryggt och säkert rätts-samhälle och en effektiv förvaltning. Även skyddet för privatlivet enligt Europakonventionen får begränsas för vissa närmare angivna ändamål men bara i den utsträckning inskränkningarna är nödvän-diga i ett demokratiskt samhälle. Motsvarande begränsningar får göras enligt EU:s stadga för de grundläggande rättigheterna.

Europadomstolen har i sin praxis slagit fast att artikel 8 i Europa-konventionen ålägger staten såväl en negativ förpliktelse att avstå från att göra intrång i rätten till respekt för privat- och familjelivet som en positiv förpliktelse att skydda enskilda mot att andra enskil-da handlar på ett sätt som innebär integritetsintrång (se t.ex. Airey mot Irland, dom den 9 oktober 1979, § 32, Serie A nr 32 och X och Y mot Nederländerna, dom den 26 mars 1985, § 23, Serie A nr 91).

Tidigare och pågående utredningar om integritetsskydd

År 1966 fick Integritetsskyddskommittén (Ju 1967:62) i uppdrag att utreda förutsättningarna för ett stärkt skydd på personrättens om-råde. Arbetet, som redovisades i fyra betänkanden (Skydd mot avlyss-ning, SOU 1970:47, Fotografering och integritet, SOU 1974:85, Re-klam och integritet, SOU 1976:48 och Privatlivets fred, SOU 1980:8),

resulterade bl.a. 1975 i lagstiftning om straff för olovlig avlyssning och 1977 i lagstiftning om TV-övervakning (i nuvarande lagstiftning benämnd kamera-övervakning). Frågor om skydd mot intrång i privatlivet har därefter även behandlats av bl.a. Yttrandefrihetsutredningen (Värna yttrandefriheten, SOU 1983:70), Data- och offentlighetskommittén (Integritetsskyddet i informationssamhället 3. Grundlagsfrågor, Ds Ju 1987:8), Personnummerutredningen (Personnummer – integritet och effektivitet, SOU 1994:63), Datalagskommittén (Integritet – Offentlighet – Informationsteknik, SOU 1997:39) och Utredningen om integritetsskydd i arbetslivet (Integritetsskydd i arbetslivet, SOU 2009:44). Detta utredningsarbete har bl.a. resulterat i en grundlagsändring 1989 (tidigare 2 kap. 3 § andra stycket RF) och införandet av personuppgiftslagen 1998. I maj 2013 beslutade regeringen direktiv till en särskild utredare (A 2013:04) som bl.a. ska undersöka i vilken utsträckning och av vilka skäl arbetsgivare begär att få se utdrag ur belastningsregistret från arbetssökande och i vilken utsträckning det förekommer att arbetsgivare begär att redan anställda visar upp sådana registerutdrag (dir. 2013:56). Uppdraget ska redovisas senast den 30 april 2014.

Regeringen beslutade i april 2004 direktiv till en parlamenta-risk kommitté, Integritetsskyddskommittén (Ju 2004:05), med uppdrag att kartlägga och analysera sådan lagstiftning som rör den personliga integriteten, att överväga om regeringsformens bestämmelse om skydd för den personliga integriteten i 2 kap. 3 § andra stycket borde ändras samt att överväga om det vid sidan av befintlig lagstiftning borde finnas generellt tillämpliga bestämmelser till skydd för den personliga integriteten. Kartläggnings- och analysuppdraget redovisades i betänkandet Skyddet för den personliga integriteten – Kartläggning och analys (SOU 2007:22). I sitt slutbetänkande Skyddet för den personliga integriteten – Bedömningar och förslag (SOU 2008:3) redovisade kommittén bl.a. förslag till ett stärkt grundlagsskydd för den personliga integriteten och ett förslag om straff för viss fotografering och filmning. Betänkandets förslag har hittills lett till införandet av bestämmelsen i 2 kap. 6 § andra stycket RF (prop. 2009/10:80, bet. 2009/10:KU19, rskr. 2009/10:304, bet. 2010/11:KU4, rskr. 2010/11:21) och till införande av ett nytt brott i 4 kap. brottsbalken, kränkande fotografering (prop. 2012/13:69, bet. 2012/13:JuU21, rskr. 2012/13:250).

I sitt slutbetänkande framhöll Integritetsskyddskommittén att det finns mycket som talar för att det i Sverige borde inrättas en ordning som innebär att regeringen genom en skrivelse årligen informerar riksdagen om utvecklingen i fråga om integritetsskyddet (SOU 2008:3 s. 326). Kommittén ansåg också att det fanns skäl att överväga en utveckling och breddning av Datainspektionens funktioner. Kommittén ansåg att uppgiften inte borde vara begränsad till området för elektroniska data eller till teknikutvecklingen som sådan utan omfatta också teknikens tillämpning i människornas vardag (bet. s. 332). Vidare bedömde kommittén att det kunde finnas skäl att i en framtid överväga inrättandet av ett särskilt integritetsskyddsråd med ett brett uppdrag att vaka över integritetsskyddet i dess helhet (bet. s. 335).

Senare års utveckling

Historiskt sett har det konstitutionella skyddet för den personliga integriteten – vid sidan av skyddet för den kroppsliga integriteten – i allt väsentligt inskränkt sig till att begränsa det allmännas utrymme att ingripa mot den fria åsiktsbildningen som en av grundvalarna för ett demokratiskt styrelseskick (prop. 2009/10:80 s. 176). Rättsutvecklingen under senare år visar dock att synen på skyddet för enskildas privatliv har för-ändrats och att detta intresse numera betonas starkare än tidigare. I förarbetena till 2 kap. 6 § andra stycket RF framhålls att respekten för individens självbestämmande är grundläggande i en demokrati (prop. 2009/10:80 s. 176). Förstärkningen av grundlagsskyddet för den personliga integriteten innebär således att vikten av individens självbestämmande nu betonas tydligare än tidigare i grundlag.

Frågor som rör skyddet för den personliga integriteten har vidare under senare år fått förhållandevis stort utrymme i den allmänna debatten om statens möjligheter att använda olika tekniska hjälpmedel i syfte att förebygga, utreda och lagföra brott. Detta gäller t.ex. i fråga om möjligheterna att använda hemlig rumsavlyssning (s.k. buggning) och hemlig övervakning och avlyssning av elektronisk kommunikation samt lagring av trafikdata från mobiltrafik och internetanvändning för brottsbekämpande syften. Signalspaning i försvarsunderrättelseverksamhet är ett annat område som har varit föremål för debatt. Frågor om skydd för den personliga integriteten har i denna lagstiftning varit grundläggande för ett system med tydliga tillstånds- och kontrollmekanismer.

Enskildas användning av internet har ökat stadigt under hela 2000-talet. Den mängd information som är tillgänglig på internet har ökat explosionsartat. Den är lättillgänglig – bl.a. genom användning av effektiva sökmotorer – och i stor utsträckning helt kostnadsfri. En betydande del av informationen har också tillkommit genom enskildas användning av internet, snarare än genom traditionella mediekanaler.

Alla myndigheter använder i dag informationsteknik. I princip all framställning av information hos myndigheterna sker på elektronisk väg och utbyte av uppgifter mellan myndigheter sker i stor utsträckning elektroniskt. Ett omfattande förvaltningspolitiskt reformarbete pågår i syfte att effektivisera förvaltningen bl.a. genom att utveckla den s.k. elektroniska förvaltningen (e-förvaltning).

Integritetsrisker i både offentlig och privat verksamhet

Enskilda har ofta små möjligheter att påverka vilka uppgifter som statliga och kommunala myndigheter får tillgång till om dem själva. Hanteringen av informationen sker vanligen på villkor som utesluter den enskildes inflytande över vilka uppgifter som behandlas. Möjligheterna att få uppgifter raderade är normalt sett mycket begränsade när uppgifterna förekommer i allmänna handlingar. Den mängd av uppgifter som totalt sett förekommer i verksamheten är också mycket stor. Det är mot bakgrund av detta viktigt att säkerställa respekten för den personliga integriteten inom ramen för den verksamhet som det allmänna ansvarar för.

Regeringens ambition är att Sverige ska vara en av de ledande nationerna i världen när det gäller e-förvaltning. En väl fungerande e-förvaltning kan både bidra till en effektiv hushållning med statens medel och erbjuda medborgarna en hög servicenivå i kontakterna med myndigheterna. Tekniska lösningar som tas fram inom e-förvaltningsarbetet kan bidra till att skyddet för den personliga integriteten stärks, bl.a. genom att de personuppgifter som myndigheterna har att hantera i sina verk-samheter hålls korrekta och aktuella. En del integritetsrisker kan också minimeras genom god användning av tekniska lösningar för säkert informationsutbyte mellan myndigheter. E-legitimation kan användas för att öka spårbarheten i sökningar. En ökad samordning av myndigheternas informationshantering kan dock

samtidigt innebära ökade integritetsrisker. Motsvarande risker kan även uppkomma när privata företag utvecklar affärsprocesser och samordnar sin datalagring.

Det samlade intrång i den skyddade personliga sfären som uppkommer som en följd av olika åtgärder, processer och övervakning som enskilda utsätts för i dagens samhälle är inte bara ett resultat av verksamhet som det allmänna ansvarar för. Enskilda utsätts i hög grad även för intrång i den personliga integriteten från andra enskilda. Användningen av internet som kanal för informationsspridning har skapat tidigare oanade möjligheter att utnyttja yttrandefriheten för att nå ut till andra med tankar och idéer eller med information som kan väcka debatt i viktiga samhällsfrågor. Men internet kan också användas av dem som vill sprida information i vida kretsar i syfte att skada andra. Personuppgifter som är lättillgängliga på internet kan också användas i bedrägligt syfte genom identitetsstölder och liknande. Tillgången till information kan även leda till särskilda risker för individer som har ett behov av skydd för sina personuppgifter på grund av att det finns en fara för att de utsätts för trakasserier, hot och våld.

Inom arbetslivet gäller att en arbetsgivare har rätt att, inom ramen för anställningsavtalet, bestämma bl.a. vilka åtgärder som ingår i arbetsuppgiften, hur arbetet ska utföras och var detta ska ske. En arbetstagare måste i princip följa en arbetsledningsorder, i vart fall så länge den anvisade åtgärden inte strider mot lag eller god sed på arbetsmarknaden eller annars är att anse som otillbörlig. Det innebär bl.a. att en arbetstagare i viss utsträckning kan behöva finna sig i att godta en övervaknings- eller kontrollåtgärd från arbetsgivarens sida. För att bedöma vad som är god sed när det gäller utövandet av kontrollåtgärder måste dock normalt en avvägning göras mellan arbetsgivarens intresse av åtgärden och arbetstagarens intresse av skydd för den personliga integriteten. Åtgärden kan vara tillåtlig på denna grund bara om den är proportionerlig i förhållande till sitt syfte.

Överenskommelse om en ny utredning

Hösten 2011 träffades mellan regeringen och Socialdemokraterna en överenskommelse om att tillsätta en parlamentarisk integritetskommission. Enligt överenskommelsen ska kommissionen ha ett upp-

drag som löper under längre tid och som har ett tydligt individperspektiv. Kommissionen ska enligt överenskommelsen beakta olika former av integritetsaspekter, bl.a. sådana som kan förekomma inom sociala medier, privata företag och förvaltningsmyndigheter. Den ska också följa upp de överväganden Integritetsskyddskommittén gjorde när det gäller behovet av att inrätta ett integritetsskyddsråd.

Uppdraget att kartlägga och analysera faktiska och potentiella risker för intrång i den personliga integriteten

Möjligheterna att via internet snabbt sprida information om företeelser i omvärlden eller att dela information om egna tankar och idéer med en stor krets människor skapar ovärderliga möjligheter för enskilda att utnyttja sin informations- och yttrandefrihet. Stora mängder data kan nu överföras på mycket kort tid. Den snabba tekniska utvecklingen på it-området har bidragit till detta. Samtidigt har kostnaderna för denna hantering minskat, vilket gör att såväl myndigheter som privata företag sett möjligheter till nya sätt att bedriva och effektivisera sin verksamhet. I detta ingår exempelvis kartläggning av enskildas beteendemönster på internet för att skapa nya affärsmöjligheter. Även om ett visst företag inte har tekniska eller administrativa möjligheter att göra detta i egen regi finns det företag som säljer tjänster som ger tillgång till beräkningskapacitet, datalagring och analysfunktioner över internet, s.k. molntjänster. De nya möjligheterna innebär samtidigt nya utmaningar och risker bland annat för intrång i den personliga integriteten.

Enskilda använder i stor utsträckning sociala medier, t.ex. Facebook, Instagram och Twitter, där de offentliggör potentiellt integritetskänsligt material som kan få stor och oförutsedd spridning. Det kan vara svårt för enskilda att bilda sig en upp-fattning om omfattningen av behandlingen av deras personliga uppgifter efter sådan publicering och spridning. Detta väcker frågor bl.a. om vem som har rätt till uppgifterna när de väl har publicerats och hur enskilda bör gå till väga om de önskar få dem borttagna.

Integritetsskyddskommittén (Ju 2004:05) redovisade i betänkandet Skyddet för den personliga integriteten – Kartläggning och analys (SOU 2007:22) en omfattande kartläggning och analys av sådan lagstiftning som berör den personliga integriteten. Uppdraget utfördes utifrån ett utpräglat lagstiftningsperspektiv. Vidare omfattade kart-

läggningen och analysen endast sådan verksamhet som bedrivs enbart av det allmänna eller av både det allmänna och enskilda, t.ex. skola, sjukvård, och forskning, och inte sådan verksamhet som i första hand endast bedrivs av enskilda aktörer. Någon mer ingående undersökning av vad senare års teknikutveckling och teknikanvändning som helhet inneburit i fråga om riskerna för integritetsintrång för enskilda individer har inte gjorts.

Mot bakgrund av samhälls- och teknikutvecklingen under senare år finns nu behov av att genomföra en kartläggning och analys av sådana faktiska eller potentiella risker för intrång i den personliga integriteten som kan finnas vid användning av informationsteknik i både privat och offentlig verksamhet. En sådan kartläggning bör göras med utgångspunkt i ett tydligt individperspektiv. I detta ligger att alla slags åtgärder som kan påverka enskilda individer från integritetssynpunkt bör kartläggas. Att kartläggningen ska göras utifrån ett utpräglat individperspektiv innebär också att kommittén bör analysera riskerna för intrång i den personliga integriteten på ett samlat sätt ur den enskildes synvinkel och att bedömningarna inte begränsas till att enbart avse tydligt avgränsade verksamheter eller situationer. I det sammanhanget bör särskilt beaktas vilka möjligheter privatpersoner har att själva bestämma över hur information om dem används och vidareförmedlas för användning i annan verksamhet än den ursprungligen är avsedd för.

Inom ramen för kartläggningen bör en uppföljning göras av hur den reform av grundlagsskyddet för den personliga integriteten, som trädde i kraft 2011, har fallit ut. Uppföljningen bör innefatta en kartläggning och analys av de integritetsaspekter som aktualiserats i lagstiftningsarbetet sedan den nya grundlagsbestämmelsen trädde i kraft. Om kommittén med anledning av vad den kommer fram till i sin kartläggning och analys bedömer att det finns behov av att kartlägga och analysera även sådan lagstiftning som tillkommit dessförinnan kan kommittén förorda tilläggsdirektiv. I analysen av de potentiella riskerna för intrång i den personliga integriteten vid användningen av modern informationsteknik bör hänsyn även tas till de fördelar som användningen av sådan teknik kan ha i både offentlig och privat verksamhet.

Uppdraget

Kommittén ska utifrån ett individperspektiv kartlägga och analysera sådana faktiska och potentiella risker för intrång i den personliga integriteten som kan finnas i samband med användning av informationsteknik. Kommittén ska vid kartläggningen och analysen beakta risker för intrång genom åtgärder såväl från andra individer och företag som från det allmännas sida. I uppdraget ingår att belysa eventuella skillnader ur ett könsperspektiv. Inom ramen för kartläggningen ska kommittén även följa upp och analysera effekterna i lagstiftningsarbetet av den förstärkning av grundlagsskyddet för den personliga integriteten som skedde genom lagstiftning som trädde i kraft 2011.

Uppdraget att överväga inrättandet av ett integritetsskyddsråd

Det finns för närvarande en rad myndigheter som har till uppgift att tillvarata enskildas intresse av skydd för den personliga integriteten. Datainspektionen har det övergripande ansvaret att värna skyddet för enskilda vid behandling av personuppgifter. Inspektionen har också ett övergripande tillsynsansvar när det gäller kameraövervakning enligt kameraövervakningslagen (2013:460). Även länsstyrelserna har ansvar för tillsyn över kameraövervakning, men det ansvaret begränsar sig till övervakning på platser dit allmänheten har tillträde. Post- och telestyrelsen har i uppdrag att utöva tillsyn vid behandling av uppgifter vid elektronisk kommunikation. Tillsyn över behandlingen av personuppgifter utövas på vissa särskilda områden även av andra myndigheter. Det finns inte något enskilt statligt organ som har ett bredare och mera övergripande uppdrag att följa utvecklingen på integritetsskyddsområdet.

Regeringen anser att det, i linje med vad Integritetsskyddskommittén tidigare framfört (SOU 2008:3 s. 335), nu finns anledning att överväga och ta ställning till värdet och behovet av att ge en myndighet ett brett och samlat uppdrag att följa utvecklingen på området för den personliga integriteten. Om ett sådant behov bedöms finnas ska kommittén överväga om det är lämpligast att för detta ändamål inrätta ett särskilt integritetsskyddsråd eller om ett sådant uppdrag i stället bör anförtros en befintlig myndighet. Kommittén ska föreslå en lösning som är så kostnadseffektiv som möjligt och där överlappande ansvar och dubbelarbete i möjligaste mån undviks.

Vid sina överväganden ska kommittén beakta samhälls- och teknikutvecklingen i stort, särskilt de faktiska och potentiella risker för intrång i den personliga integriteten som kommitténs uppdrag omfattar.

Uppdraget

Kommittén ska, med beaktande av samhälls- och teknikutvecklingen i stort och mot bakgrund av slutsatserna av sitt kartläggnings- och analysuppdrag följa upp betänkandet Skyddet för den personliga integriteten (SOU 2008:3) när det gäller behovet av att inrätta ett integritetsskyddsråd och särskilt överväga om de uppgifter som ett sådant råd i så fall bör ges lämpligen kan fullgöras av en befintlig myndighet, samt föreslå nödvändiga författningsändringar.

Uppdragets genomförande och konsekvensbeskrivningar

Kommittén ska följa samhällsdebatten på integritetsskyddsområdet och bedriva sitt arbete utåtriktat och inhämta synpunkter från berörda intressenter i samhället, t.ex. genom att anordna hearings. Kommittén ska samråda med E-delegationen (Fi 2009:01), Datainspektionen, Post- och telestyrelsen och andra berörda myndigheter samt med arbetsmarknadens parter och med andra berörda organisationer. I sitt arbete ska kommittén följa utvecklingen av förhandlingarna inom EU med reformeringen av den unionsrättsliga dataskyddsregleringen. Kommittén ska även följa arbetet inom Regeringskansliet med de förslag som Utredningen om registerutdrag i arbetslivet (A 20013:04) senare kommer att redovisa för regeringen (dir. 2014:34).

Inom Regeringskansliet pågår ett arbete med att se över den straffrättsliga lagstiftning som syftar till att skydda enskilda mot hot och andra fridskränkningar bl.a. på internet. Kommittén ska följa hur detta arbete fortlöper.

Om regeringen beslutar att ge en utredning i uppdrag att utreda frågor med anknytning till kommitténs uppdrag att överväga frågor som rör den personliga integriteten, ska kommittén samråda med den utredningen.

I uppdraget ingår inte att föreslå ändringar i grundlag.

Kommittén ska i enlighet med vad som föreskrivs i kommittéförordningen (1998:1474) redovisa konsekvenserna av sina förslag och vid behov föreslå hur dessa ska finansieras.

Redovisning av uppdraget

Uppdraget ska redovisas slutligt senast den 1 december 2016. Kommittén får, om den bedömer att det är lämpligt, lämna ett eller flera delbetänkanden.

(Justitiedepartementet)

Kommittédirektiv 2016:12

Tilläggsdirektiv till Integritetskommittén (Ju 2014:09)

Beslut vid regeringssammanträde den 18 februari 2016

Förlängd tid för och ändring av uppdraget

Regeringen beslutade den 8 maj 2014 kommittédirektiv om den personliga integriteten (dir. 2014:65). I uppdraget ingår bl.a. att utifrån ett individperspektiv kartlägga och analysera sådana faktiska och potentiella risker för intrång i den personliga integriteten som kan uppkomma i samband med användning av informationsteknik i såväl privat som offentlig verksamhet och att, med beaktande av samhälls- och teknikutvecklingen i stort och mot bakgrund av slutsatserna av kartläggnings- och analysuppdraget, följa upp betänkandet Skyddet för den personliga integriteten (SOU 2008:3) när det gäller behovet av att inrätta ett integritetsskyddsråd. Enligt utredningens direktiv skulle uppdraget redovisas senast den 1 december 2016.

Utredningstiden förlängs. Uppdraget ska i stället redovisa ett delbetänkande senast den 31 maj 2016 som omfattar dels kartläggningen och analysen av riskerna för integritetsintrång, dels behovet av att inrätta ett integritetsskyddsråd. Uppdraget i övrigt ska redovisas senast den 1 juni 2017.

(Justitiedepartementet)

Statens offentliga utredningar 2017

Kronologisk förteckning

1. För Sveriges landsbygder – en sammanhållen politik för arbete, hållbar tillväxt och välfärd. N.
2. Kraftsamling för framtidens energi. M.
3. Karens för statsråd och statssekreterare. Fi.
4. För en god och jämlik hälsa. En utveckling av det folkhälsopolitiska ramverket. S.
5. Svensk social trygghet i en globaliserad värld. Del 1 och 2. S.
6. Se barnet! Ju.
7. Straffprocessens ramar och domstolens beslutsunderlag i brottmål – en bättre hantering av stora mål. Ju.
8. Kunskapsläget på kärnavfallsområdet 2017. Kärnavfallet – en fråga i ständig förändring. M.
9. Det handlar om oss. – unga som varken arbetar eller studerar. U.
10. Ny ordning för att främja god sed och hantera oredlighet i forskning. U.
11. Vägskatt. Volym 1 och 2. Fi.
12. Att ta emot människor på flykt. Sverige hösten 2015. Ju.
13. Finansiering av infrastruktur med privat kapital? Fi.
14. Migrationsärenden vid utlandsmyndigheterna. Ju.
15. Kvalitet och säkerhet på apoteksmarknaden. S.
16. Sverige i Afghanistan 2002–2014. UD.
17. Om oskuldspresumtionen och rätten att närvara vid rättegången. Genomförande av EU:s oskuldspresumtionsdirektiv. Ju.
18. En nationell strategi för validering. U.
19. Uppdrag: Samverkan. Steg på vägen mot fördjupad lokal samverkan för unga arbetslösa. A.
20. Tillträde för nybörjare – ett öppnare och enklare system för tillträde till högskoleutbildning. U.
21. Läs mig! Nationell kvalitetsplan för vård och omsorg om äldre personer. Del 1 och 2. S.
22. Från värdekedja till värdecykel – så får Sverige en mer cirkulär ekonomi. M.
23. digitalforvaltning.nu. Fi.
24. Ett arbetsliv i förändring – hur påverkas ansvaret för arbetsmiljön? A.
25. Samlad kunskap – stärkt handläggning. S.
26. Delningsekonomi. På användarnas villkor. Fi.
27. Vissa frågor inom fastighets- och stämpelskatteområdet. Fi.
28. Ett nationellt centrum för kunskap om och utvärdering av arbetsmiljö. A.
29. Brottsdatalag. Ju
30. En omreglerad spelmarknad. Del 1 och 2. Fi.
31. Stärkt konsumentskydd på bostadsrättsmarknaden. Ju.
32. Substitution i Centrum – stärkt konkurrenskraft med kemikaliesmarta lösningar. M.
33. Stärkt ställning för hyresgäster. Ju.
34. Ekologisk kompensation – Åtgärder för att motverka nettoförluster av biologisk mångfald och ekosystemtjänster, samtidigt som behovet av markexploatering tillgodoses. M.
35. Samling för skolan. Nationell strategi för kunskap och likvärdighet. U.
36. Informationssäkerhet för samhällsviktiga och digitala tjänster. Ju.
37. Kvalificerad välfärdsbrottslighet – förebygga, förhindra, upptäcka och beivra. Ju.

38. Kvalitet i välfärden – bättre upphandling och uppföljning. Fi.
39. Ny dataskyddslag. Kompletterande bestämmelser till EU:s dataskyddsförordning. Ju.
40. För dig och för alla. S.
41. Meddelarskyddslagen – fler verksamheter med stärkt meddelarskydd. Ju.
42. Vem har ansvaret? M.
43. På lika villkor! Delaktighet, jämlikhet och effektivitet i hjälpmedelsförsörjningen. S.
44. Entreprenad, fjärrundervisning och distansundervisning. U.
45. Ny lag om företagshemligheter. Ju.
46. Stärkt ordning och säkerhet i domstol. Ju.
47. Nästa steg på vägen mot en mer jämlik hälsa. Förslag för ett långsiktigt arbete för en god och jämlik hälsa. S.
48. Kunskapsbaserad och jämlik vård. Förutsättningar för en lärande hälso- och sjukvård. S.
49. EU:s dataskyddsförordning och utbildningsområdet. U.
50. Personuppgiftsbehandling för forskningsändamål. U.
51. Utbildning, undervisning och ledning – reformvård till stöd för en bättre skola. U.
52. Så stärker vi den personliga integriteten. Ju.

Statens offentliga utredningar 2017

Systematisk förteckning

Svensk social trygghet i en globaliserad värld. Del 1 och 2.[5]

Kvalitet och säkerhet på apoteksmarknaden. [15]

Läs mig! Nationell kvalitetsplan för vård och omsorg om äldre personer. Del 1 och 2. [21]

Samlad kunskap – stärkt handläggning. [25]

För dig och för alla. [40]

På lika villkor! Delaktighet, jämlikhet och effektivitet i hjälpmedelsförsörjningen. [43]

Nästa steg på vägen mot en mer jämlik hälsa. Förslag för ett långsiktigt arbete för en god och jämlik hälsa. [47]

Kunskapsbaserad och jämlik vård. Förutsättningar för en lärande hälso- och sjukvård. [48]

Utbildningsdepartementet

Det handlar om oss. – unga som varken arbetar eller studerar. [9]

Ny ordning för att främja god sed och hantera oredlighet i forskning. [10]

En nationell strategi för validering [18]

Tillträde för nybörjare – ett öppnare och enklare system för tillträde till högskoleutbildning. [20]

Samling för skolan. Nationell strategi för kunskap och likvärdighet. [35]

Entreprenad, fjärrundervisning och distansundervisning. [44]

EU:s dataskyddsförordning och utbildningsområdet. [49]

Personuppgiftsbehandling för forskningsändamål.[50]

Utbildning, undervisning och ledning – reformvård till stöd för en bättre skola. [51]

Utrikesdepartementet

Sverige i Afghanistan 2002–2014. [16]