Datainspektionen

Yttrande
2017-09-04

Diarienr
1210-2017

Ert diarienr
Ju2017/04264/L6

Justitiedepartementet
Regeringskansliet
103 33 STOCKHOLM

Remittering av betänkandet SOU 2017:39 Ny dataskyddslag

Datainspektionen har granskat betänkandet utifrån inspektionens uppgift att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter. Med anledning av antalet frågor som behandlas i betänkandet begränsar sig Datainspektionens yttrande till frågor av väsentlig betydelse för den enskildes personliga integritet.

Datainspektionen tillstyrker generellt utredningens förslag att införa en till dataskyddsförordningen kompletterande dataskyddslag. Inspektionen lämnar dock följande synpunkter i särskilda frågor.

5 Ett nytt svenskt regelverk om dataskydd

5.2 Överväganden och förslag

Utredningen föreslår i betänkandet att en ny lag och förordning som kompletterar dataskyddsförordningen på ett generellt plan ska införas. Utredningen betonar att författningarna dock inte är heltäckande och endast utgör ett komplement till dataskyddförordningen. Datainspektionen anser, i likhet med utredningen, att det är bra att den nya lagen därför i författningsförslaget benämns lagen med *kompletterande* bestämmelser till EU:s dataskyddsförordning.

Enligt Datainspektionen är det ett faktum, vilket även utredningen anger, att den föreslagna kompletterande dataskyddslagen endast reglerar vissa specifika frågor. Användningen av benämningen dataskyddslagen kan dock ge intrycket av att den utgör en sådan heltäckande generell dataskyddslagstiftning som personuppgiftslagen utgör idag. Till skillnad från förhållandet mellan dataskyddsdirektivet och personuppgiftslagen ska

dataskyddsförordningen från och med den 25 maj 2018 utgöra den primära och generella regleringen av behandling av personuppgifter. För att inte riskera att vilseleda den enskilde tillämparen bör den föreslagna lagen enligt Datainspektionens mening konsekvent benämnas den *kompletterande dataskyddslagen*.

Dataskyddsförordningen är direkt tillämplig men har en direktivliknande karaktär, det vill säga den kräver i vissa fall kompletterande nationell lagstiftning. Detta faktum tillsammans med att den föreslagna kompletterande dataskyddslagen endast reglerar vissa begränsade frågor medför enligt Datainspektionen att behandlingar av personuppgifter kan komma att sakna rättsligt stöd när dataskyddsförordningen ska börja tillämpas. Om det inte säkerställs att särskild nationell lagstiftning införs där behov finns och dataskyddsförordningen så kräver, finns det risk för att behandling av personuppgifter av vikt för samhällets funktioner inte kan utföras.

7 Förhållande till yttrande- och informationsfriheten

Datainspektionen ifrågasätter om utredningens förslag till bestämmelser om dataskyddsförordningens och den föreslagna kompletterande dataskyddslagens förhållande till tryckfrihetsförordningen och yttrandefrihetsgrundlagen är förenlig med EU-rätten. Inspektionen föreslår därför att bestämmelsen i 1 kap. 4 § första stycket i den föreslagna kompletterande dataskyddslagen utgår.

Utredningen föreslår en bestämmelse i 1 kap. 4 § första stycket i den kompletterande dataskyddslagen som anger att bestämmelserna i dataskyddsförordningen och i denna lag inte ska tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefriheten i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. I avsnitt 7.4 i utredningsbetänkandet framgår att utredningen avsett att det ska utgöra en upplysningsbestämmelse motsvarande den i 7 § första stycket personuppgiftslagen.

Som den föreslagna bestämmelsen är utformad framstår den inte som en ren upplysningsbestämmelse. Att ha en bestämmelse som den i

personuppgiftslagen som upplyser om principen om lex superiori, dvs. att grundlag går före vanlig lag, är en sak. I detta fall är förhållandena annorlunda eftersom det rör sig om en reglering av förhållandet till direkt tillämplig EU-rättslig lagstiftning. Ordalydelsen i den föreslagna bestämmelsen anvisar att svenska grundlagsbestämmelser i tryckfrihetsförordningen och yttrandefrihetsgrundlagen äger företräde framför EU-rätt, dvs. att bestämmelser i dataskyddsförordningen inte ska tillämpas vid en konflikt. Det kan inte sägas vara en korrekt beskrivning av rättsläget. Den direkt tillämpliga artikel 85 i dataskyddsförordningen anger för övrigt att medlemsstaterna i lag ska förena rätten till integritet i enlighet med denna förordning med yttrande- och informationsfriheten, inbegripet behandling som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande. Dataskyddsförordningen ger således inte utrymme för ett sådant generellt undantag i nationell lag som utredningen enligt bestämmelsens ordalydelse föreslår. Att dataskyddsförordningen i artikel 86 innehåller ett mer generellt undantag för offentlighetsprincipen är en annan sak. Det ska dock framhållas att utredningen heller inte gör gällande att det ingått i dess uppdrag att närmare analysera förhållandet mellan grundlagsskyddet för informations- och yttrandefriheten och rätten till skydd av personuppgifter enligt dataskyddsförordningen.

Förhållandet mellan det särskilda grundlagsskyddet för tryck- och yttrandefriheten i tryckfrihetsförordningen och yttrandefrihetensgrundlagen å ena sidan och skyddet för den personliga integriteten i personuppgiftslagen och dataskyddsdirektivet å andra sidan har diskuterats vid ett flertal tillfällen (se sammanställning i SOU 2016:58 s. 386).

Datainspektionen har påpekat de risker för integritetsskyddet som grundlagsskyddet i tryckfrihetsförordningen och yttrandefrihetsgrundlagen medför, särskilt vad gäller personuppgiftsbehandling som sker på internet och som omfattas av utgivningsbevis för databaser enligt 1 kap. 9 § andra stycket yttrandefrihetsgrundlagen, senast i Datainspektionens yttrande den 20 december 2016 över Mediegrundlagsutredningens betänkande SOU 2016:58 (Datainspektionens dnr 1908-2016).

Datainspektionen anser att det, även med hänsyn tagen till det undantag i tryckfrihetsförordningen och yttrandefrihetsgrundlagen som har föreslagits av Mediegrundlagsutredningen (SOU 2016:58 s. 375 f), kvarstår konflikter med integritetsskyddet. Mediegrundlagsutredningens förslag omfattar endast

uppgiftssamlingar med känsliga personuppgifter och uppgifter om lagöverträdelser och gäller endast uppgiftssamlingar som tillhandahålls på ett visst sätt. Det är vanligt att uppgifter om privatpersoner hämtade från allmänna handlingar som har begärts ut från myndigheter tillhandahålls i mycket omfattande databaser med stöd av utgivningsbevis enligt yttrandefrihetsgrundlagen. Dessa databaser får anses vara sådana ”rena personregister” som Konstitutionsutskottet vid införandet om bestämmelserna om utgivningsbevis befarade att grundlagsskyddet skulle komma att omfatta (2001/02:21KU s. 32).

Att Sverige har en skyldighet att förena rätten till integritet enligt dataskyddsförordningen med yttrande- och informationsfriheten följer som nämnts av artikel 85 i dataskyddsförordningen. Enligt Datainspektionen kan denna skyldighet inte tolkas så att viss behandling av personuppgifter helt undantas bestämmelserna i dataskyddsförordningen, vilket blir fallet om man anser att bestämmelserna i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen alltid ges företräde vid en eventuell konflikt med dataskyddsförordningen. Eftersom det är två grundläggande rättigheter som ska vägas mot varandra ska det enligt praxis från EU-domstolen och Europadomstolen vara möjligt att göra en proportionalitetsbedömning i det enskilda fallet.

I de fall då yttrande- och informationsfrihetsintresset är relativt svagt jämfört med integritetsskyddet, såsom vid publicering av stora databaser med personuppgifter på internet måste det finnas utrymme för att i det enskilda fallet tillämpa bestämmelserna i dataskyddsförordningen. Det gäller särskilt med tanke på att Sverige har en långtgående offentlighetsprincip som möjliggör insamling av personuppgifter till sådana databaser.
Det kan noteras att Europadomstolen den 27 juni 2017 avkunnade en dom (Case of Satakunnan Markkinapörssi OY and Satamedia OY v. Finland, no. 931/13) som har betydelse i detta sammanhang. Domen gäller den personuppgiftsbehandling som förekom i samband med att två finska bolag publicerade taxeringsuppgifter avseende större delen av Finlands befolkning. Den avgörande frågan var om yttrande- och informationsfrihetsintresset skulle få väga över i en proportionalitetsbedömning mot integritetsskyddet. Bolagens verksamhet hade tidigare varit under prövning av EU-domstolen (Satakunnan C-73/07 ECLI:EU:C:2007:506). EU-domstolen konstaterade att den aktuella personuppgiftsbehandlingen ska anses utgöra behandling för journalistiska ändamål m.m. ”om denna verksamhet endast syftar till att

sprida information, åsikter eller idéer till allmänheten, vilket det ankommer på den nationella domstolen att bedöma". Den finska Högsta förvaltningsdomstolen (HFD:2009:82) som hade begärt förhandsavgörandet från EU-domstolen gjorde bedömningen att bolagens personuppgiftsbehandling inte omfattades av undantaget i artikel 9 i dataskyddsdirektivet för bland annat journalistiska ändamål. Det beslut som därefter fattades av finska dataskyddsmyndigheten överklagades av bolagen. Efter att bolagens yrkande om upphävande av dataskyddsmyndighetens beslut avslogs i de finska domstolarna, väckte bolagen talan mot Finland i Europadomstolen för överträdelse av artikel 10 i Europakonventionen. Europadomstolen konstaterade att finska Högsta förvaltningsdomstolens dom inte innebar någon överträdelse av artikel 10 i Europakonventionen. Domstolen ansåg att den finska Högsta förvaltningsdomstolen hade gjort en korrekt bedömning i intresseavvägningen mellan skyddet för privatlivet och rätten till yttrandefrihet. I bedömningen tog Europadomstolen hänsyn till att konventionsstaterna "enjoyed wide margin of appreciation in deciding how to strike a fair balance between the respective rights under Articles 8 and 10 of the Convention in this case" (p. 195). I denna bedömning måste dock beaktas "the fact that [the] State, somewhat exceptionally, as a matter of constitutional choice and, in the interests of transparency, has chosen to make taxation data accessible to the public" (p.195).

Enligt Datainspektionen kan Europadomstolens dom tolkas så att om konventionsstaterna tillåter en vid öppenhet till personuppgifter som behandlas av myndigheter måste detta val (constitutional chocie) uppvägas av ett integritetsskydd som innebär att myndigheter och domstolar i de enskilda fallen ska kunna göra en proportionalitetsbedömning som står i överensstämmelse med Europadomstolens praxis. Att som i Sveriges fall kombinera en omfattande offentlighet till allmänna handlingar med ett starkt grundlagsskydd för yttrandefriheten som möjliggör publicering av omfattande samlingar av personuppgifter utan något direkt journalistiskt ändamål och utan annat integritetsskydd än det som följer av tryck- och yttrandefrihetsbrotten, framstår inte som förenligt med Europakonventionen. Samma bedömning torde gälla enligt dataskyddsförordningen och EU:s stadga om de grundläggande rättigheterna.

Mot denna bakgrund bedömer Datainspektionen att det finns tillfällen då grundlagsskyddet i tryckfrihetsförordningen och yttrandefrihetsgrundlagen inte kan ges företräde framför bestämmelserna i dataskyddsförordningen.

Mot denna bakgrund föreslår Datainspektionen att den av utredningen föreslagna bestämmelsen i den kompletterande dataskyddslagens 1 kap. 4 § utgår.

8 Rättslig grund för behandling av personuppgifter

8.3 Överväganden och förslag

Datainspektionen anser att ett författningsförslag avseende artiklarna 6. 1 c och e i dataskyddsförordningen, för att vara förtydligande, i vart fall bör ange att kraven i artikel 6.3 måste följas. Datainspektionen tillstyrker därför inte förslagen i den kompletterande dataskyddslagens 2 kap. 3-4 §§ i sin nuvarande utformning.

Datainspektionen anser att den rättsliga grunden för myndigheters administrativa åtgärder måste klargöras i det fortsatta lagstiftningsarbetet.

Dataskyddsförordningen innebär att all svensk lagstiftning på dataskyddsområdet måste följa dataskyddsförordningen när denna lagstiftning faller in under förordningens tillämpningsområde. Vid normkonflikter mellan förordningens bestämmelser och nationell lag äger förordningen företräde framför nationell rätt i enlighet med principen om EU-rättens företräde. Förordningen blir således det primära regelverket avseende behandling av personuppgifter.

Enligt skäl 8 i förordningen får medlemsstaterna införliva delar av förordningen i nationell rätt i den utsträckning det är nödvändigt för samstämmigheten och för att göra de nationella bestämmelserna begripliga. Datainspektionen anser att det i dessa fall måste stå helt klart för tillämparna att sådana bestämmelser endast är ett återgivande av bestämmelserna i förordningen och att det är förordningens bestämmelser som ska tillämpas.

Utredningen har i avsnittet analyserat dels vad som kan anses som grunden för behandlingen enligt artikel 6.1 c och e, dels vad som menas med att denna grund ska vara fastställd i nationell rätt. Enligt utredningens bedömning medför kravet i dataskyddsförordningen att grunden för behandlingen ska fastställas inte att det krävs en särskild reglering med anledning av förordningen. Det finns dock enligt utredningen anledning att i den

kompletterande dataskyddslagen som föreslås tydliggöra på vilka sätt rättslig förpliktelse, myndighetsutövning och uppgift av allmänt intresse kan utgöra rättslig grund för behandling av personuppgifter. Ett sådant förtydligande är enligt utredningen förenligt med unionsrätten.

Mot bakgrund av den faktiska utformningen av lagförslaget i den kompletterande dataskyddslagens 2 kap. 3-4 §§ ifrågasätter Datainspektionen om dessa bestämmelser kan anses utgöra enbart ett återgivande av de regler som gäller direkt enligt artikel 6.1 c och e i förordningen. Det kan ifrågasättas om angivande av kollektivavtal generellt som en rättslig grund i de aktuella paragraferna kan anses följa direkt av dataskyddsförordningen. De aktuella paragraferna ger dessutom i sin nuvarande utformning intryck av att i sig utgöra en rättslig grund för behandling av personuppgifter. Ett införlivande av förordningens regler i nationell rätt på ett sätt som inte leder till ökad tydlighet utan snarare riskerar att missleda den personuppgiftsansvarige är inte förenligt med skäl 8 i förordningen.

Förändringen av dataskyddsregleringen från ett genom personuppgiftslagen implementerat dataskyddsdirektiv till en direkt tillämplig dataskyddsförordning innebär en pedagogisk utmaning. De personuppgiftsansvariga som ska tillämpa förordningen måste förstå att de ska pröva sin behandling av personuppgifter primärt mot dataskyddsförordningen i sin helhet. En sådan bedömning gällande laglig behandling av personuppgifter enligt artikel 6.1 c och e, omfattar då inte endast att hitta t.ex. en tillämplig författning som kan utgöra rättslig grund för behandlingen, utan innebär även en bedömning av om denna författning uppfyller kraven bl.a. på tydlighet, precisering och förutsägbarhet i skäl 41 samt kraven på proportionalitet i artikel 6.3 andra stycket sista meningen. Det är inte möjligt att, som utredningen synes göra i betänkandet (s. 128 f.), presumera att de åtgärder som myndigheterna vidtar i syfte att utföra sina uppdrag och åligganden och som antagits i enlighet med grundlagens bestämmelser om normgivningskompetens och kommunalt självstyre i sig har en legal grund som offentliggjorts genom tydliga, precisa och förutsägbara regler och som därmed uppfyller kraven i skäl 41. Det är i förhållande till nödvändig behandling av personuppgifter som den rättsliga grunden ska vara tydlig och precis och dess tillämpning förutsägbar för personer som omfattas av den, i enlighet med rättspraxis vid EU-domstolen och Europeiska domstolen för de mänskliga rättigheterna. Många författningar är av naturliga skäl antagna utan att deras tydlighet, precisering och förutsägbara

tillämpning avseende behandling av personuppgifter har bedömts. Det blir därför den personuppgiftsansvariges ansvar att pröva sin behandling mot kraven i dataskyddsförordningen, oavsett vad som framgår av nationell kompletterande lagstiftning. Det måste enligt Datainspektionens mening klargöras betydligt tydligare än vad som idag kan utläsas i den föreslagna kompletterande dataskyddslagens 2 kap. 3-4 §§.

Ett författningsförslag avseende artikel 6. 1 c och e i dataskyddsförordningen bör för att vara förtydligande i vart fall ange att kraven i artikel 6.3 måste följas. Det måste vara tydligt för den enskilde tillämparen att behandlingen av personuppgifter i varje enskilt fall ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas. Datainspektionen kan därför inte tillstyrka förslagen i sin nuvarande utformning.

Utredningen har kommit till slutsatsen att artikel 6.1 andra stycket som anger att intresseavvägning (artikel 6.1 f) inte gäller för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter, innebär att myndigheter inte heller kan åberopa intresseavvägning när myndigheten behandlar personuppgifter för sina administrativa åtgärder. I betänkandet (s. 129) hänvisas i en fotnot till Artikel 29-gruppens yttrande 6/2014 om den registeransvariges berättigade intressen enligt artikel 7 i direktivet. Artikel 29-gruppen har i sitt yttrande även blickat framåt och resonerat kring hur förslaget i förordningen kan komma att påverka myndigheters användning av berättigat intresse. Artikel 29-gruppen konstaterar att *”[o]m denna bestämmelse antas och tolkas på ett sätt som innebär att offentliga myndigheter helt utesluts från att använda berättigat intresse som rättslig grund måste grunderna ”allmänt intresse” och ”myndighetsutövning” i artikel 7 e tolkas på samma sätt som förordning (EG) nr 45/2001 för närvarande tolkas, nämligen på ett sådant sätt att de offentliga myndigheterna ges en viss grad av flexibilitet, åtminstone så att myndigheternas förvaltning och funktion säkerställs.”* Artikel 29-grupen fortsätter emellertid och uttrycker att *”[a]lternativt kan sista meningen i artikel 6.1 f i förslaget till förordning tolkas så, att den inte helt och hållet utesluter offentliga myndigheter från att använda berättigat intresse som rättslig grund. I så fall bör ”behandling som utförs av myndigheter i deras myndighetsutövning” i den föreslagna artikel 6.1 f tolkas restriktivt. En sådan strikt tolkning skulle innebära att sådan behandling som behövs för dessa offentliga myndigheters förvaltning och funktion inte omfattas av ”behandling som utförs av myndigheter i deras myndighetsutövning”. Behandling som krävs för dessa offentliga myndigheters*

förvaltning och funktion skulle dock fortfarande vara möjlig inom ramen för grunden berättigat intresse."

Datainspektionen har förståelse för att det kan utgöra ett allmänt intresse att myndigheter även kan vidta administrativa åtgärder, men Datainspektionen har svårt att se att dessa alltid kan anses vara fastställda i enlighet med unionsrätten eller den nationella rätten. Det ska också beaktas att den rättsliga grunden i enlighet med skäl 41 ska vara tydlig, precis och förutsägbar. Datainspektionen är av uppfattningen att en rättslig grund som uppfyller dessa krav vanligtvis inte finns för många av de administrativa åtgärder som naturligt behövs för en fungerande verksamhet. Hur ska exempelvis personalaktiviteter rymmas inom det som är fastställt i nationell rätt? I Artikel 29-gruppens yttrande anges inledningsvis (s. 3) att intresseavvägningen kan, under rätt förhållanden samt med förbehåll för tillräckliga skyddsåtgärder, bidra till att förhindra en övertro på andra rättsliga grunder. Datainspektionen delar denna uppfattning. När det ställs krav på en rättsliga grund är det således viktigt att det finns en i korrekt ordning fattad reglering eller beslut som för såväl den registrerade, som för verksamheten, utgör en tydlig grund för den behandling av personuppgifter som utförs. Datainspektionen anser att antingen behöver myndigheters administrativa åtgärder ges en i nationell rätt fastställd rättslig grund som uppfyller kraven i skäl 41 eller så bör artikel 6.1 andra stycket tolkas såsom Artikel 29-gruppen uttrycker alternativt, det vill säga att det som behövs för offentliga myndigheters förvaltning och funktion inte ingår i den behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter. Eftersom detta avser en väsentlig mängd personuppgifter som behandlas dagligen inom offentlig verksamhet är det av stor vikt att detta klargörs i det fortsatta lagstiftningsarbetet.

9 Barns samtycke som rättslig grund

Datainspektionen avstyrker utredningens förslag, i den kompletterande dataskyddslagens 2 kap. 2 §, att som villkor för barns eget samtycke avseende informationssamhällets tjänster ange åldersgränsen till 13 år.

Datainspektionen anser inte att utredningens betänkande ger tillräckligt underlag för ställningstagandet att 13 år är en lämplig ålder med hänsyn tagen

till barns särskilda behov av skydd i samband med behandling av personuppgifter vid tillhandahållande av informationssamhällets tjänster. Datainspektionen anser att den av inspektionen hittills tillämpade tumregeln om 15 år, som en åldersgräns för när barn normalt ska anses förstå innebörden av samt konsekvenserna av en viss behandling av personuppgifter och därmed kunna ge sitt samtycke till den, är en lämplig utgångspunkt för en nationell reglering av när behandling av personuppgifter som rör ett barn ska kunna stödjas på samtycke enligt artikel 6.1 a i dataskyddsförordningen. Den uppfattningen vinner även stöd av vad Barnombudsmannen framfört till utredningen. Samtidigt ska sägas att frågan från ett integritetsskyddsperspektiv är komplicerad då det, som Statens medieråd anger, även finns en risk för att bestämmelsen i artikel 8.1 kan leda till ytterligare behandling av barns personuppgifter om åldersverifieringar skapas. En annan aspekt, som kanske inte avser rent integritetsskyddande intressen, är den harmoniseringstanke som genomsyrar dataskyddsreformen. Det senare talar för ett behov av att EU:s medlemsstater bör komma fram till en enhetligt nationell reglering av åldersgränsen för barns samtycke i samband med behandling av personuppgifter vid tillhandahållande av informationssamhällets tjänster.

Datainspektionen avstyrker därför utredningens förslag att, med avvikelse från den 16-årsgräns som dataskyddsförordningen anger, som villkor för barns eget samtycke avseende informationssamhällets tjänster nationellt bestämma åldersgränsen till 13 år.

10 Känsliga personuppgifter

10.3 Vad betyder kravet på stöd i nationell rätt

Datainspektionen anser att det utgör en brist i utredningen att det inte gjorts någon analys av hur de föreslagna undantagsbestämmelserna för behandling av känsliga personuppgifter förhåller sig kravet på rättslig grund enligt artikel 6.

Dataskyddsförordningens artikel 9.1 anger ett generellt förbud mot att behandla vissa särskilda kategorier av personuppgifter, s.k. känsliga personuppgifter. Förbudet kompletteras med en rad undantag i artikel 9.2

som möjliggör behandling av känsliga personuppgifter i vissa särskilda fall. Vissa av dessa undantag kräver att lagstiftningsåtgärder vidtas för att undantagen ska vara tillämpliga.

Utredningen har bedömt att kravet på stöd i nationell rätt i vissa av undantagen som räknas upp i artikel 9.2 medför att dessa undantag bör föreskrivas i nationell rätt tillsammans med en reglering av lämpliga skyddsåtgärder. I utredningens redogörelse för sin bedömning tas emellertid inte med det faktum att undantagen från förbudet i artikel 9.1, som antingen gäller direkt enligt förordningen eller kommer att vara reglerad i nationell rätt, endast är undantag från det generella förbudet mot att behandla känsliga personuppgifter. En behandling av personuppgifter, oavsett om de är att anse som känsliga eller inte, måste dessutom alltid ha en rättslig grund i förordningens artikel 6. Om medlemsstaterna särskilt reglerar behandlingen av personuppgifter i nationell rätt med stöd av artikel 6.1 c och e måste dessutom denna reglering följa relevanta krav i artikel 6.2 och 6.3. Av särskild vikt är kravet på proportionalitet i artikel 6.3 andra stycket sista meningen. I betänkandet anges att även om viss behandling av känsliga personuppgifter är tillåten enligt den föreslagna kompletterande dataskyddslagen måste den i det enskilda fallet också uppfylla dataskyddsförordningens krav i övrigt, exempelvis kraven i artikel 5. Någon analys av hur dessa författningsreglerade undantag förhåller sig till kravet på rättslig grund enligt artikel 6 har dock inte gjorts för något av de i betänkandet föreslagna undantagen, vilket enligt Datainspektionen utgör en brist i utredningen.

10.6 Viktigt allmänt intresse

Datainspektionen anser att författningsförslaget i den kompletterande dataskyddslagens 3 kap. 3 § bör utformas så att det klart framgår att behandling av känsliga personuppgifter enligt dessa undantagsbestämmelser endast är tillåten om behandlingen är nödvändig med hänsyn till *ett viktigt allmänt intresse*. Undantagsbestämmelsen i samma paragrafs punkt 2 bör formuleras så att behandling får ske om uppgifterna lämnats till en myndighet eller likställt organ och behandlingen krävs för hanteringen av allmänna handlingar. Begreppet absolut nödvändig i samma paragrafs punkt 3 bör enligt Datainspektionen inte användas. Istället kan det exempelvis formuleras så att behandling får ske i enstaka fall om det är av synnerlig vikt för ändamålet med behandlingen. Datainspektionen avstyrker författningsförslaget i sin nuvarande utformning.

Utredningen har gjort bedömningen att särskilda undantag från förbudet mot behandling av känsliga personuppgifter bör göras för myndigheter med stöd av artikel 9. 2 g, att behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse. På denna grund har utredningen föreslagit att myndigheter ska få behandla känsliga personuppgifter i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det. Datainspektionen ifrågasätter om den föreslagna utformningen av undantaget kan anses uttrycka det krav på ett viktigt allmänt intresse som framgår av dataskyddsförordningens artikel 9.2. g. För att behandla dessa särskilda kategorier av personuppgifter som anses särskilt känsliga för den enskildes integritet krävs att behandlingen är nödvändig inte enbart med hänsyn till ett allmänt intresse utan dessutom ett *viktigt* allmänt intresse. Detta framgår direkt av dataskyddsförordningen och ska tillämpas av den enskilde personuppgiftsansvarige oavsett vad som framgår av den kompletterande dataskyddslagen. Om denna särskilda förutsättning för behandlingen inte framgår av den föreslagna undantagsbestämmelsen finns enligt Datainspektionen risk för att myndigheter kommer behandla personuppgifter i strid med de direkta kraven i artikel 9.2 g på grund av att de vilseleds av formuleringen i den kompletterande dataskyddslagen, särskilt som det inte finns någon egentlig begränsning av vad myndigheter kan behandla som ärende.

Utredningen har vidare föreslagit att myndigheter och andra organ som omfattas av offentlighetsprincipen ska få behandla känsliga personuppgifter om de har lämnats till myndigheten eller organet och behandlingen krävs enligt lag. Skälen enligt utredningen för ett sådant undantag är att viss behandling av känsliga personuppgifter är oundviklig i myndigheternas verksamhet som en direkt följd av exempelvis tryckfrihetsförordningens, offentlighets- och sekretesslagens och förvaltningslagens krav på myndigheters och likställda organs hantering av inkomna handlingar. Datainspektionen håller med utredningen om att myndigheters hantering av inkomna handlingar torde utgöra ett sådant viktigt allmänt intresse som anges i artikel 9.2 g. Sådan behandling av känsliga personuppgifter som kan anses nödvändig för att kunna ta emot och hantera dessa handlingar torde dessutom i normalfallet uppfylla kravet på proportionalitet i nämnda artikel. Det aktuella författningsförslaget i den kompletterande dataskyddslagen anger emellertid att känsliga personuppgifter får behandlas av en myndighet om uppgifterna lämnats till myndigheten och behandlingen krävs enligt lag. Lagtexten begränsar sig således inte till lagstiftning avseende offentlighetsprincipen och myndigheters och likställda organs hantering av inkomna handlingar utan är betydligt mer öppen. Med en sådan öppen utformning av det föreslagna undantaget blir det, enligt Datainspektionens mening, inte möjligt att göra den i undantaget i artikel 9.2. g stadgade proportionalitetsbedömningen. För att uppnå det som utredningen har avsett och som de har bedömt proportionerligt krävs att författningsförslaget begränsas till den lagstiftning som reglerar myndigheters och likställda organs hantering av inkomna handlingar.

I betänkandet föreslås ett särskilt stöd för myndigheters behandling av känsliga personuppgifter i enstaka fall, om det är absolut nödvändigt för ändamålet med behandlingen och behandlingen inte innebär ett otillbörligt intrång i den registrerades personliga integritet. Användningen av begreppet absolut nödvändigt ska enligt utredningen markera restriktivitet och ska inte förväxlas med det unionsrättsliga begreppet nödvändigt. Datainspektionen anser att användningen i lagtext av två mycket likalydande begrepp, nödvändigt och absolut nödvändigt, vars betydelse väsentligen skiljer sig åt inte är lämpligt. Enligt Datainspektionens erfarenhet har enskilda personuppgiftsansvariga redan idag svårt att förstå den unionsrättsliga betydelsen av begreppet nödvändigt då denna skiljer sig från svenskt språkbruk. Att då införa ett nytt begrepp, absolut nödvändigt, vars ordalydelse endast skiljer sig från begreppet nödvändigt genom tillägg av vad som synes

vara en förstärkning, riskerar att leda till förvirring hos den enskilde personuppgiftsansvarige och en felaktig tillämpning av dataskyddsregleringen.

Datainspektionen anser således att den föreslagna författningstexten i 3 kap. 3 § bör utformas så att det klart framgår att behandling av känsliga personuppgifter enligt dessa undantagsbestämmelser endast är tillåten om behandlingen är nödvändig med hänsyn till *ett viktigt allmänt intresse*. Undantagsbestämmelsen i punkten 2 bör formuleras så att behandling får ske om uppgifterna lämnats till en myndighet eller likställt organ och behandlingen krävs för hanteringen av allmänna handlingar. Begreppet absolut nödvändig i punkten 3 bör enligt Datainspektionen inte användas. Istället kan det exempelvis formuleras så att behandling får ske i enstaka fall om det är av synnerlig vikt för ändamålet med behandlingen. Datainspektionen avstyrker författningsförslaget i sin nuvarande utformning.

10.7 Hälso- och sjukvård och social omsorg

Datainspektionen anser att det skyndsamt bör utredas huruvida den behandling av personuppgifter som sker idag inom hälso- och sjukvård och social omsorg är förenlig med artikel 9.2 h och 9.3 i dataskyddsförordningen, eller om det behöver införas en lagstadgad tystnadsplikt för de personuppgiftsbiträden som idag inte omfattas av en sådan.

I den föreslagna kompletterande dataskyddslagen föreslås en bestämmelse, 3 kap 5 §, som i princip överensstämmer med lydelsen i artikel 9.2 h i dataskyddsförordningen. Den generella bestämmelsen införs med motiveringen att det är av stor vikt att förutsättningarna för att behandla känsliga personuppgifter för hälso- och sjukvårdsändamål är reglerade på ett så tydligt sätt som möjligt. Datainspektionen delar uppfattningen att det är viktigt att områden som rör hälso- och sjukvård och social omsorg har bra och tydliga förutsättningar för sin behandling av personuppgifter. Det är särskilt viktigt eftersom det handlar om känsliga personuppgifter och berör många människor. Datainspektionen är därför oroad över att kraven på lagreglerad tystnadsplikt för den som behandlar dessa uppgifter enligt artikel 9.3 inte analyserats och omhändertagits i betänkandet. Istället hänvisas till att bestämmelsen är direkt tillämplig och att den närmare innebörden av kravet

på tystnadsplikt ytterst får uttolkas av EU-domstolen (s.185 f.). Datainspektionen delar inte den uppfattningen utan anser att regleringen av en tystnadsplikt som uppfyller kraven i artikel 9.3 måste ske i nationell rätt.

Formuleringen i artikel 9.3, att uppgifterna ska behandlas av eller under ansvar av en yrkesutövare som omfattas av tystnadsplikt, kan uppfattas så att det är tillräckligt att den personuppgiftsansvarige omfattas av en lagreglerad tystnadsplikt. Gränsen för personuppgiftsansvaret och ansvaret för sekretessen skiljer sig emellertid åt, vilket bland annat framgår i JO:s beslut från den 9 september 2014, dnr 3032-2011. JO konstaterar i beslutet att utlämnande av journaluppgifter till ett personuppgiftsbiträde eller personal hos biträdet ska prövas på vanligt sätt enligt offentlighets- och sekretesslagen. JO:s bedömning i ärendet var att vårdgivaren i det fallet inte hade rättsligt stöd för att lämna ut sekretessbelagda uppgifter om patienter då mottagaren endast omfattades av en avtalsreglerad tystnadsplikt.

Efter JO:s beslut uppstod en debatt om myndigheters möjlighet att anlita personuppgiftsbiträde om det innebär att sekretessbelagda uppgifter lämnas ut. Frågan har bland annat utretts av Pensionsmyndigheten i regeringsuppdraget ”Molntjänster i staten En ny generation av outsourcing” avsnitt 11.5 och bilaga ”Juridisk analys av myndigheters informationshantering i molnet”. Pensionsmyndigheten konstaterar i sin rapport, på samma sätt som JO, att offentlighets- och sekretesslagens bestämmelser kan hindra myndigheter från att lämna ut vissa typer av sekretessbelagda uppgifter till privata it-leverantörer eftersom det saknas straffrättsligt sanktionerade tystnadsplikter för anställda hos dessa aktörer. Pensionsmyndigheten ger i sin slutsats i rapporten åtta förslag till regeringen varav ett av förslagen är att utreda närmare om det är lämpligt och ändamålsenligt att införa en lagreglerad och straffsanktionerad tystnadsplikt för privata leverantörer av it-tjänster.

Inom vårdområdet är det många privata aktörer som levererar it-tjänster och på så sätt behandlar stora mängder personuppgifter i egenskap av personuppgiftsbiträde. Med anledning av kravet på lagstadgad tystnadsplikt enligt artikel 9.3 dataskyddsförordningen för att få behandla personuppgifter inom vårdområdet, ifrågasätter Datainspektionen om dessa leverantörer kan behandla personuppgifterna utan att en lagreglerad sekretess gäller för deras behandling.

Datainspektionen har i en skrivelse till Justitiedepartementet den 7 juli 2017, Datainspektionens dnr 1704-2017, (http://www.datainspektionen.se/Documents/2017-07-13-skrivelse-sekretess.pdf) bl.a. angett att det skyndsamt bör utredas huruvida den behandling av personuppgifter som sker idag inom hälso- och sjukvård och social omsorg, med omfattande outsourcing, är förenlig med artikel 9.2 h och 9.3 i dataskyddsförordningen, eller om det behöver införas en lagstadgad tystnadsplikt de personuppgiftsbiträden som idag inte omfattas av en sådan.

11 Personuppgifter som rör lagöverträdelser

Datainspektionen anser att det i det fortsatta lagstiftningsarbetet bör tas fram vägledning för när det kan vara motiverat att i enskilda fall låta andra än myndigheter behandla uppgifter om lagöverträdelser.

Av artikel 10 i dataskyddsförordningen följer att behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder endast får utföras under kontroll av myndighet eller då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs.

Utredningen har i betänkandet angett att artikel 10 öppnar upp för en reglering som inte längre uttrycks som ett generellt förbud att behandla uppgifter om lagöverträdelser med möjligheter till undantag, på det sätt som 21 § personuppgiftslagen utformats. Enligt förslaget föreskrivs i stället att sådana uppgifter får behandlas av myndigheter samtidigt som Datainspektionen även fortsättningsvis ska få besluta i enskilda fall att andra än myndigheter får behandla sådana uppgifter. Enligt utredningen är det naturligt att utrymmet för att tillåta andra än myndigheter att behandla uppgifter om lagöverträdelser blir något mindre begränsat än tidigare.

Datainspektionen delar utredningens uppfattning att utformningen av artikel 10 kan tolkas som att Datainspektionen i viss mån kan vara något mindre restriktiv än tidigare med att i enskilda fall tillåta andra än myndigheter att behandla uppgifter om lagöverträdelser. Datainspektionen anser att detta förhållande bör belysas närmare i det fortsatta lagstiftningsarbetet.

Datainspektionen efterlyser därför mer vägledning, såsom konkreta exempel, för när det kan vara motiverat att i enskilda fall låta andra än myndigheter behandla uppgifter om lagöverträdelser.

14 Arkiv och statistik

14.4.2 Rättslig grund och tillåten vidarebehandling

Datainspektionen anser att det föreslagna bemyndigandet innebär att regeringen och Riksarkivet kan ge enskilda arkiv rätt att behandla personuppgifter för arkivändamål av allmänt intresse trots att en sådan uppgift inte är fastställd i nationell rätt. Eftersom ett sådant fastställande är en förutsättning för att behandlingen ska ha en rättslig grund enligt artikel 6.1 e finns inget stöd för att som utredningen har föreslagit endast reglera behandlingen av personuppgifter. Datainspektionen avstyrker därför förslaget i 2 kap. 5 § i den kompletterande dataskyddslagen.

I betänkandet anges att den rättsliga grunden enligt artikel 6.1 e för behandling av personuppgifter utgörs av den uppgift av allmänt intresse som är fastställd i svensk rätt och inte av själva behandlingen som sådan. Utredningen har vidare konstaterat att enskilda arkivinstitutioner utanför arkivlagstiftningens tillämpningsområde riskerar att sakna en rättslig grund för sin behandling av personuppgifter. För att dessa institutioner ska kunna utföra sin arkivverksamhet, som i normalfallet torde vara att anse som en uppgift av allmänt intresse i dataskyddsförordningens mening, krävs därför att uppgiften fastställs i svensk rätt.

Vad utredningen föreslår är emellertid inte att *uppgiften* för enskilda arkivinstitutioner ska kunna fastställas av regering respektive Riksarkivet. I författningsförslaget i den kompletterande dataskyddslagens 2 kap. 5 § anges i stället att föreskrifter eller i enskilda fall beslut om själva *behandlingen av personuppgifter* ska kunna meddelas. Medlemsstaterna har givetvis en möjlighet att med stöd av artikel 6.2 och 6.3 i särskild lagstiftning både reglera själva uppgiften av allmänt intresse samt de särskilda förutsättningar som ska gälla för behandlingen av personuppgifter. En sådan reglering måste då uppfylla de krav som anges i nämnda bestämmelser, exempelvis kravet på proportionalitet i artikel 6.3 andra stycket sista meningen. Arkiv för enskilda

aktörer kan komma att innehålla stora mängder personuppgifter som förvaras under lång tid. Det är därför av synnerligen vikt att den aktuella behandlingen av personuppgifter verkligen är nödvändig för att utföra en uppgift av allmänt intresse, att denna uppgift är fastställd i nationell rätt och dessutom proportionell mot det legitima mål som eftersträvas.

Datainspektionen anser att det föreslagna bemyndigandet innebär att regeringen och Riksarkivet kan ge enskilda arkiv rätt att behandla personuppgifter för arkivändamål av allmänt intresse trots att en sådan uppgift inte är fastställd i nationell rätt. Eftersom ett sådant fastställande är en förutsättning för att behandlingen ska ha en rättslig grund enligt artikel 6.1 e finns inget stöd för att som utredningen har föreslagit endast reglera behandlingen av personuppgifter. Datainspektionen avstyrker därför förslaget i 2 kap. 5 § i den kompletterande dataskyddslagen.

14.4.3 Förhållandet till arkivlagstiftningen och behandling av känsliga personuppgifter

Datainspektionen tillstyrker inte författningsförslaget i den kompletterande dataskyddslagens 3 kap. 6 § tredje stycke. Om en sådan delegering som där föreslås ändå anses lämplig anser Datainspektionen att den myndighet som regeringen bestämmer i vart fall ska samråda med Datainspektionen.

Utredningen anser att det faktum att behandling av känsliga personuppgifter för arkivändamål särbehandlas i artikel 9.2 j i dataskyddsförordningen talar för att all behandling av känsliga personuppgifter för arkivändamål måste omfattas av en särskild undantagsreglering för att vara tillåten. Utredningen föreslår därför en bestämmelse som anger att känsliga personuppgifter med stöd av artikel 9.2 j får behandlas för arkivändamål av allmänt intresse om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om bevarande och vård av arkiv. Regeringen eller den myndighet som regeringen bestämmer ska dessutom kunna meddela föreskrifter om undantagsreglering för enskilda arkivs behandling av känsliga personuppgifter.

Dessutom ska enligt utredningens förslag Riksarkivet kunna besluta om att enskilda arkiv ska kunna behandla känsliga personuppgifter för arkivändamål av allmänt intresse. Datainspektionen ifrågasätter om en sådan delegering till

Riksarkivet att besluta om undantag från förbudet att behandla känsliga personuppgifter verkligen kan anses uppfylla kraven på särskild undantagsreglering i enlighet med artikel 9.2 j. Utredningen har själva i avsnitt 10 avseende kravet på stöd i nationell rätt för behandling av känsliga personuppgifter angett att förordningens krav på lämpliga och särskilda skyddsåtgärder talar för att såväl undantaget som skyddsåtgärder bör regleras och även preciseras i nationell rätt. Medför delegeringen till Riksarkivet att de också ska kunna besluta om vad som är lämpliga skyddsåtgärder i dessa fall? Riksarkivet har enligt sin instruktion ett särskilt ansvar för den statliga arkivverksamheten och arkivvården i landet och ska särskilt verka för att myndigheter fullgör sina skyldigheter enligt arkivlagen, vilket naturligt bör innebära att Riksarkivet i sin roll värnar bevarandet av uppgifter. Datainspektionen kan därför inte tillstyrka författningsförslaget i den kompletterande dataskyddslagens 3 kap. 6 § tredje stycke. Om en sådan delegering som där föreslås ändå anses lämplig anser Datainspektionen att den myndighet som regeringen bestämmer i vart fall ska samråda med Datainspektionen.

14.4.4 Lämpliga skyddsåtgärder

Datainspektionen anser att utredningen inte har visat att det skydd som finns idag i nationell lagstiftning för myndigheters arkiv uppfyller kraven på lämpliga skyddsåtgärder i dataskyddsförordningens artikel 9.2 j. Datainspektionen tillstyrker därför inte lagförslaget i den kompletterande dataskyddslagens 4 kap. 1 § andra stycket.

Som lämplig skyddsåtgärd i enlighet med kraven i artikel 9.2 j har utredningen föreslagit att personuppgifter som behandlas enbart för arkivändamål av allmänt intresse inte ska få användas för att vidta åtgärder i fråga om den registrerade annat än om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen. Vad gäller myndigheters arkiv utgör de nationella författningsbestämmelserna om sekretess en särskild skyddsåtgärd som utformats efter en avvägning mellan behovet av skydd och intresset av insyn. Med anledning av detta samt att myndigheters arkiv omfattas av allmänna bestämmelser om skydd av arkiv anser utredningen att den föreslagna begränsningen inte ska hindra myndigheter från att använda personuppgifter som finns i allmänna handlingar.

Bestämmelser om sekretess kan visserligen enligt Datainspektionens mening utgöra en sådan lämplig skyddsåtgärd som avses i dataskyddsförordningen. Sekretessen är emellertid, som utredningen själva anger, ett uttryck för det skydd som behövs för att komplettera offentlighetsprincipen. Sekretessen har till uppgift att minimera den skada som ett utlämnande av allmänna handlingar kan medföra för den enskilde. Rätten till skydd för personuppgifter, där krav på skyddsåtgärder ingår, utgår från att den enskilde ska ha ett grundläggande skydd för sitt privatliv och det oavsett om den enskilde anses lida men eller inte. Sekretessen har dessutom sina begränsningar, t.ex. genom sekretessbrytande bestämmelser. Utredningen har vidare nämnt att myndigheters arkiv omfattas av allmänna bestämmelser om skydd av arkiv men har inte angett vilket skydd för personuppgifter dessa bestämmelser innebär. Sammantaget finner Datainspektionen att utredningen inte har visat att det skydd som finns idag i nationell lagstiftning för myndigheters arkiv uppfyller kraven på lämpliga skyddsåtgärder i dataskyddsförordningens artikel 9.2 j. Datainspektionen kan därför inte tillstyrka lagförslaget i den kompletterande dataskyddslagens 4 kap. 1 § andra stycket.

14.4.5 Undantag från vissa av den registrerades rättigheter

Datainspektionen anser att det är lagstiftarens uppgift att specificera de skyddsåtgärder som krävs för att undantag ska kunna göras från de registrerades rättigheter i enlighet med artikel 89.3 i dataskyddsförordningen. Att den personuppgiftsansvarige själv ska efterleva villkoren i artikel 89.1 kan inte uppfylla dessa krav. Datainspektionen avstyrker därför förslaget om ändring i arkivförordningens 7 a-d §§.

Om personuppgifter behandlas för arkivändamål av allmänt intresse får det enligt 89.3 i dataskyddsförordningen under vissa förutsättningar föreskrivas om undantag från vissa av förordningens rättigheter med förbehåll för de villkor och skyddsåtgärder som avses i artikel 89.1 I betänkandet föreslås också att undantag från dataskyddsförordningens artiklar 15, 16, 18 och 21 ska behållas och införas i arkivförordningen. Några förslag på särskilda skyddsåtgärder ges däremot inte. Utredningen har dock i betänkandet angett att de föreslagna undantagen endast kan tillämpas under förutsättning att de

direkt tillämpliga villkoren i artikel 89.1 om bl.a. skyddsåtgärder och uppgiftsminimering efterlevs.

I skäl 156 anges att medlemsstaterna bör på särskilda villkor med förbehåll för lämpliga skyddsåtgärder för de registrerade ha rätt att specificera och göra undantag från vissa av den registrerades rättigheter i samband med bl.a. behandling av arkivändamål av allmänt intresse. Det är således lagstiftarens uppgift att specificera de skyddsåtgärder som krävs för att undantag ska kunna göras från de registrerades rättigheter. Att den personuppgiftsansvarige själv ska efterleva villkoren i artikel 89.1 kan inte uppfylla kraven enligt artikel 89.3. Datainspektionen avstyrker därför förslaget om ändring i arkivförordningens 7 a-d §§.

16 Godkännande av certifieringsorgan

Datainspektionen anser att det behövs nationella bestämmelser som förtydligar och specificerar förfarandet kring ackreditering och hur den uppgiften ska fördelas mellan tillsynsmyndigheten och ett nationellt ackrediteringsorgan.

När det gäller certifiering och ackreditering av certifieringsorgan ger dataskyddsförordningen utrymme för viss flexibilitet ifråga om vem som ska göra vad. Själva utfärdandet av certifieringen kan göras av tillsynsmyndigheten eller ett certifieringsorgan enligt artikel 42.5. Medlemsstaterna ska enligt artikel 43.1 säkerställa att ett certifieringsorgan är ackrediterat av tillsynsmyndigheten, ett nationellt ackrediteringsorgan eller av båda dessa. Tillsynsmyndigheten ska göra en periodisk översyn av utfärdade certifieringar och om kraven för certifiering inte längre uppfylls ska certifieringen återkallas av tillsynsmyndigheten eller ett certifieringsorgan. Om kraven för ackreditering inte längre uppfylls ska ackrediteringen återkallas av tillsynsmyndigheten eller ackrediteringsorganet. De kriterier som en certifiering och en ackreditering ska grunda sig på ska tas fram av den nationella tillsynsmyndigheten.

När det gäller uppgiften att utfärda certifieringar och att ta fram kriterier för certifiering och ackreditering pekas den nationella tillsynsmyndigheten ut direkt i förordningen (artikel 42.5 och 43.3). När det gäller ackreditering av

certifieringsorgan ska medlemsstaterna säkerställa att dessa är ackrediterade av en eller båda av de följande, tillsynsmyndigheten och det nationella ackrediteringsorgan som utsetts enligt EU-förordningen (EG) nr 765/2008. Utredningens tolkning är att ett certifieringsorgan har en direkt på förordningen grundad rätt att få sin ackreditering gjord av tillsynsmyndigheten. Datainspektionen är av annan uppfattning. Enligt inspektionens mening överlämnar artikel 43.1 till medlemsstaterna att meddela närmare bestämmelser om vem som ska vara ackrediteringsorgan och till och med förutsätter en sådan närmare nationell reglering. Bestämmelsen i artikel 57.1 q anger visserligen att tillsynsmyndigheten ska ha till uppgift att utfärda ackreditering av certifieringsorgan men, såsom hänvisningen till artikel 43 får förstås, endast inom ramen för vad medlemsstaten har beslutat i denna fråga. Om inte bestämmelser tas fram på nationell nivå kommer det att vara oklart vem som ska kunna utfärda ackrediteringar. Datainspektionen anser därför att det behövs nationella bestämmelser som förtydligar och specificerar förfarandet kring ackreditering och hur den uppgiften ska fördelas mellan tillsynsmyndigheten och ett nationellt ackrediteringsorgan.

17 Sekretess

17.3 Sekretess hos tillsynsmyndigheten

Datainspektionen anser att det i offentlighets- och sekretesslagen ska införas en bestämmelse som innebär att absolut sekretess alternativt sekretess med omvänt skaderekvisit gäller i Datainspektionens verksamhet för anmälningar av personuppgiftsincidenter som görs i enlighet med artikel 33 i dataskyddsförordningen och för förhandssamråd som görs i enlighet med artikel 36 i dataskyddsförordningen. En sådan sekretessbestämmelse bör även omfatta anmälningar av personuppgiftsincidenter och begäran om förhandssamråd som görs i enlighet med förslaget till brottsdatalag, SOU 2017:29.

Vidare bör frågan om en sekretessbrytande reglering vid tillsynsmyndighetens internationella samarbete övervägas närmare i det fortsatta lagstiftningsarbetet.

Utredningen har gjort bedömningen att uppgifter som rör incidentrapportering enligt artikel 33 i förordningen kommer att skyddas av sekretess till skydd för säkerhets- och bevakningsåtgärder avseende system för automatiserad behandling av information i enlighet med 18 kap. 8 § offentlighets- och sekretesslagen. Utredningen hänvisar vidare till NIS-utredningens uppdrag att överväga om detta sekretesskydd för rapportering av it-incidenter är tillräckligt. I sitt betänkande föreslog emellertid inte NIS-utredningen något stärkt sekretesskydd för rapportering av it-incidenter (SOU 2017:36).

Datainspektionen har i en skrivelse till Justitiedepartementet den 7 juli 2017, Datainspektionens dnr 1704-2017, angett att vissa frågor om sekretess och tystnadsplikt med anknytning till EU:s dataskyddsreform skyndsamt måste utredas (http://www.datainspektionen.se/Documents/2017-07-13-skrivelse-sekretess.pdf).

Datainspektionen anser att en svag sekretess för uppgifter om personuppgiftsincidenter inte är tillräcklig. Syftet med dataskyddsförordningens bestämmelser om anmälan av personuppgiftsincidenter är att förmå den personuppgiftsansvarige att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig för de aktuella personuppgifterna. Den incidentrapportering som förutsätts ske kan dock i praktiken innebära en upplysning om att ingivarens it-system är sårbart för attacker. Risken för angrepp utifrån skulle kunna öka om det genom incidentrapporteringen avslöjas att den personuppgiftsansvariges it-system har brister. Datainspektionen befarar även att samma skäl kommer att påverka den personuppgiftsansvariges vilja att anmäla eller beskriva personuppgiftsincidenter i den omfattning som dataskyddsförordningen föreskriver. Risken är stor att den personuppgiftsansvarige underlåter att rapportera incidenter eller rapporterar endast övergripande eller bristfällig information. I den mån Sverige har ett svagare skydd för känslig företagsinformation än andra länder kommer de företag som står under tillsyn av den svenska dataskyddsmyndigheten dessutom riskera att hamna i en sämre situation ur konkurrenssynpunkt än företag som står under tillsyn av annat lands dataskyddsmyndighet.

Den personuppgiftsansvarige är dessutom under vissa omständigheter skyldig att göra en konsekvensbedömning avseende dataskydd enligt artikel 35 i

dataskyddsförordningen. Om en sådan konsekvensbedömning visar att personuppgiftsbehandlingen skulle leda till hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken ska den personuppgiftsansvarige enligt artikel 36 samråda med tillsynsmyndigheten före behandlingen. Datainspektionen förutsätter att sådana förhandssamråd i många fall kommer att innefatta mycket känslig och ingående information om en viss personuppgiftsansvarigs verksamhet. Datainspektionen ser även i detta fall en risk att personuppgiftsansvariga på grund av oro för att affärskritiska uppgifter ska bli offentliga väljer att utelämna viktiga delar i en konsekvensbedömning, eller helt underlåter att begära förhandssamråd.

Datainspektionen anser att det i offentlighets- och sekretesslagen ska införas en bestämmelse som innebär att absolut sekretess alternativt sekretess med omvänt skaderekvisit gäller i Datainspektionens verksamhet för anmälningar av personuppgiftsincidenter som görs i enlighet med artikel 33 i dataskyddsförordningen och för förhandssamråd som görs i enlighet med artikel 36 i dataskyddsförordningen. En sådan sekretessbestämmelse bör även omfatta anmälningar av personuppgiftsincidenter och begäran om förhandssamråd som görs i enlighet med förslaget till brottsdatalag något som Datainspektionen framfört i sitt remissyttrande över betänkandet Brottsdatalag SOU 2017:29 (Datainspektionens dnr 913-2017).

Tillämpningen av dataskyddsförordningen kan komma att innebära ett samarbete mellan tillsynsmyndigheterna. Det innebär bland annat att myndigheterna ska översända nödvändig och relevant information till varandra. För att tillsynsmyndigheten i Sverige ska få lämna ut uppgifter till andra tillsynsmyndigheter krävs en i lag reglerad uppgiftsskyldighet som bryter den i dataskyddsförordningens artikel 54.2 stadgade sekretessen för tillsynsmyndighetens ledamöter och personal. Utredningen har inte haft ett uttryckligt uppdrag att analysera behovet av en sekretessbrytande bestämmelse. Visserligen kan det hävdas att dataskyddsförordningens olika bestämmelser med krav på samarbete och informationsutbyte med andra tillsynsmyndigheter är att anse som en i lag bestämd uppgiftsskyldighet som bryter sekretessen men frågan är om denna uppgiftsskyldighet är tillräckligt tydlig. Enligt Datainspektionen behöver det övervägas närmare i det fortsatta lagstiftningsarbetet.

18 Sanktioner

18.5 Sanktionsavgifter inom offentlig sektor

Datainspektionen tillstyrker utredningens förslag att sanktionsavgifter ska få tas ut även av statliga och kommunala myndigheter.

Datainspektionen delar utredningens bedömning att sanktionsavgifter ska få tas ut även av statliga och kommunala myndigheter. Som utredningen anger måste enskildas intresse av skydd för sin personliga integritet väga lika tungt oavsett om uppgifter behandlas i det allmännas verksamhet som i den privata sektorn. Datainspektionen delar också, utifrån myndighetens erfarenheter på tillsynsområdet, utredningens uppfattning att myndigheter inte heller i större utsträckning än privata personuppgiftsansvariga kan förväntas följa dataskyddsregleringen. Det bör även tilläggas att det inom offentligt finansierad vård, omsorg och utbildning finns en betydande andel privata utförare som behandlar personuppgifter i sin verksamhet och som således är personuppgiftsansvariga. Sanktionsavgifter bör även av detta skäl kunna tas ut såväl från myndigheter som från privata subjekt. Datainspektionen tillstyrker därför utredningens förslag.

20 Ikraftträdande- och övergångsbestämmelser

20.3 Överväganden och förslag

Datainspektionen avstyrker övergångsbestämmelsernas punkter 3, 4 och 7.

Utredningen föreslår i betänkandet övergångsbestämmelser som bl.a. anger att personuppgiftslagen ska fortsätta gälla i den utsträckning som det i annan lag eller förordning finns bestämmelser som innehåller hänvisningar till lagen. Äldre föreskrifter ska även gälla för ärenden hos Datainspektionen som inletts men inte avgjorts före ikraftträdandet.

Dataskyddsförordningen är direkt tillämplig och dess bestämmelser ska börja tillämpas från och med den 25 maj 2018 på all pågående behandling av personuppgifter. Enligt Datainspektionen kan ett införande av de föreslagna övergångsbestämmelserna ovan därför medföra vissa problem vid

tillämpningen. Behandling av personuppgifter är i de allra flesta fall en pågående aktivitet. Från och med den 25 maj 2018 ska en sådan pågående behandling bedömas enligt regleringen i dataskyddsförordningen, oavsett om ett ärende inletts hos Datainspektionen innan denna tidpunkt. Detta gäller även om det för en viss typ av behandling finns särskilda regler i annan lag eller förordning som hänvisar till personuppgiftslagen.

Dataskyddsförordningen innebär att det inom det område som regleras av förordningen inte är möjligt att i nationell rätt ha andra bestämmelser om dataskydd än sådana kompletterande bestämmelser som antas med stöd av förordningen. Personuppgiftslagen grundar sig på dataskyddsdirektivet och kompletterar därför inte dataskyddsförordningen. Som de föreslagna övergångsbestämmelserna är utformade kan de komma att ange personuppgiftslagen som tillämplig lag trots att behandlingen ska bedömas enligt dataskyddsförordningen och dess kompletterande bestämmelser. Eftersom dataskyddsförordningen i sådana fall alltid har företräde kan de föreslagna övergångsbestämmelserna komma att bli vilseledande.

I betänkandet föreslås att den straffrättsliga regleringen upphävs samt att det i övergångsbestämmelserna anges att äldre föreskrifter ska gälla för överträdelser som skett före ikraftträdandet. Bestämmelserna i dataskyddsförordningen och den föreslagna kompletterande dataskyddslagen innebär att straffet ersätts med administrativa sanktionsavgifter. Utredningen har bedömt att trots att dessa formellt sett får anses lindrigare så kan kraftfulla sanktionsavgifter i många fall anses som en svårare sanktion än ett bötesstraff. Utredningen menar därför att den föreslagna övergångsbestämmelsen inte strider mot principen om lindrigaste lag enligt 2 kap. 10 § regeringsformen eller 5 § andra stycket lagen om införande av brottsbalken och hänvisar till ett lagrådsyttrande gällande administrativa sanktionsavgifter för yrkesfiskare (s. 344). Datainspektionen ifrågasätter denna jämförelse. För överträdelse vid yrkesfiske är enbart vissa handlanden avkriminaliserade, straffbestämmelser finns fortfarande kvar och i båda fallen synes reaktionerna träffa yrkesfiskaren själv. Överträdelser av dataskyddsregler avkriminaliseras däremot enligt utredningens förslag. Det innebär att istället för att en fysisk person straffas kommer en administrativ sanktionsavgift kunna tas ut av en personuppgiftsansvarig alternativt ett personuppgiftsbiträde, vilka i princip alltid är juridiska personer. För den fysiska personen leder betänkandets förslag till frihet från straff vilket måste anses som en lindrigare reaktion än enligt nuvarande lagstiftning.

Datainspektionens anser att utredningen inte visat att det i detta fall är möjligt att frångå gällande bestämmelser rörande principen om lindrigaste lag.

Datainspektionen avstyrker därför övergångsbestämmelsernas punkter 3, 4 och 7.

Detta yttrande har beslutats av tf generaldirektören Eva Håkansson efter föredragning av juristen Ulrika Harnesk. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom, enhetschefen Katarina Tullstedt samt juristerna Martin Brinnen, Elisabeth Jilderyd, Hans Kärnlöf och Agneta Runmarker deltagit.

Eva Håkansson

Ulrika Harnesk