Stockholm den 7 september 2017

R-2017/0906

Till Justitiedepartementet

Ju2017/04264/L6

Sveriges advokatsamfund har genom remiss den 15 maj 2017 beretts tillfälle att avge yttrande över betänkandet Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning (SOU 2017:39).

Sammanfattning

Advokatsamfundet har i huvudsak ingen erinran mot förslagen i betänkandet, med undantag för nedan angivna påpekanden. För det fall inte annat anges är alla referenser till kapitel och paragrafer i detta remissvar referenser till förslaget till dataskyddslag.

Utsträckt tillämpningsområde för dataskyddsförordningen

I 1 kap. 2 § anges att ”*[b]estämmelserna i dataskyddsförordningen, i den ursprungliga lydelsen, och i denna lag ska i tillämpliga delar gälla även vid behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten och i verksamhet som omfattas av avdelning V kapitel 2 i fördraget om Europeiska unionen”.* Även om Advokatsamfundet förstår svårigheten i att analysera vilka artiklar och kapitel i dataskyddsförordningen som inte ska tillämpas vid behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten, och i verksamhet som omfattas av avdelning V kapitel 2 i fördraget om Europeiska unionen, är det från ett legalitetsperspektiv otillfredsställande att inte på förhand veta vilka bestämmelser i dataskyddsförordningen som ska och inte ska tillämpas. Det är otillfredsställande att det i varje enskilt fall ska göras en bedömning om förordningens bestämmelser går att tillämpa. Advokatsamfundet förordar därför att det i dataskyddslagen preciseras vilka artiklar och kapitel som inte ska tillämpas inom de här angivna områdena.

Advokatsamfundet vill också påpeka, med hänvisning till vad som anförts i föregående stycke, att enligt artikel 2.2 b i dataskyddsförordningen ska inte förordningen tillämpas på behandling av personuppgifter som medlemsstaterna utför när de bedriver verksamhet som omfattas av avdelning V kapitel 2 i EU-fördraget, dvs. den gemensamma utrikes- och säkerhetspolitiken (GUSP). Dataskyddsutredningen anger på sidan 90 att rättsgrunden för dataskyddsförordningen är artikel 16 i fördraget om Europeiska unionens funktionssätt. Det man däremot inte analyserar eller ens nämner i utredningen är artikel 39 i EU-fördraget. Enligt artikel 39 kan rådet anta beslut om bestämmelser om skydd för enskilda personer i fråga om behandling av personuppgifter i medlemsstaterna, när dessa utövar verksamhet som omfattas av kapitlets tillämpningsområde, dvs. GUSP, samt om den fria rörligheten av sådana uppgifter. Det är därför vanskligt att nu utöka dataskyddsförordningens tillämpning till detta område då denna svenska lagstiftning, utökningen av dataskyddsförordningens tillämpningsområde genom dataskyddslagen, kan komma att strida mot framtida bestämmelser beslutade av rådet.

Avvikande bestämmelser i annan författning

I 1 kap. 3 § anges att *”om en annan lag eller en förordning innehåller någon bestämmelse som rör behandling av personuppgifter och som avviker från denna lag tillämpas den bestämmelsen”*. Detta innebär att om speciallagstiftning innehåller bestämmelser som avviker från dataskyddslagen ska dessa bestämmelser tillämpas. Eftersom dataskyddsförordningen har direkt effekt borde det av denna bestämmelse framgå att bestämmelser som avviker från dataskyddslagen ska tillämpas såvida de inte är oförenliga med dataskyddsförordningen. Med den föreslagna bestämmelsen framgår det explicit att speciallagstiftning ska gälla före dataskyddslagen, men inte att dataskyddsförordningen, inom dess tillämpningsområde och inom det område där medlemsstaterna inte har en nationell regleringsmöjlighet, gäller före såväl dataskyddslagen som speciallagstiftning rörande personuppgifter.

Tystnadsplikt för dataskyddsombud

Regleringen i 1 kap. 6 § innebär att tystnadsplikt gäller för dataskyddsombud. När det gäller sekretess för dataskyddsombud anser Advokatsamfundet att utredningens förslag inte är tillräckliga för att uppfylla förordningens krav på tystnadsplikt för dataskyddsombud inom offentlig verksamhet. Sekretess gäller av varierande styrka inom olika verksamheter och hos olika myndigheter. I betänkandet behandlas dock inte frågan om att skyldigheten att se till att dataskyddsombudet är bundet av sekretess varierar beroende på inom vilken verksamhet vederbörande fullgör sina uppgifter. Enligt Pensionsmyndighetens mening (se deras remissvar daterat den 23 augusti 2017, sidan 7) kan ett sådant resonemang ha två principiella utgångspunkter. Enligt den första utgångspunkten ska sekretessintresset bedömas utifrån myndighetens kärnverksamhet. Enligt den andra utgångspunkten ska bedömningen utgå från den verksamhet som bedrivs av dataskyddsombudet. Enligt Pensionsmyndighetens uppfattning, vilken delas av Advokatsamfundet, talar principiella skäl för att det är det senare synsättet som ska tillämpas, innebärande att samma skyddsintresse gäller inom alla verksamheter. En sådan ordning framstår, såsom

Pensionsmyndigheten framhåller i sitt remissvar, som enklare lagstiftningstekniskt och mer förutsebar för dem som sekretessen ska skydda. Samma tystnadsplikt som gäller inom den privata sektorn bör således gälla för det allmänna, se mer i stycket nedan.

I 1 kap. 6 § första stycket regleras tystnadsplikten för dataskyddsombud inom den privata sektorn. Där framgår att ”*[d]en som utsetts till dataskyddsombud enligt artikel 37 i dataskyddsförordningen får inte obehörigen röja det som han eller hon vid fullgörandet av sin uppgift har fått veta om enskilds personliga och ekonomiska förhållanden”.* Dataskyddsförordningen ger ingen närmare vägledning om vad som ska omfattas av dataskyddsombudets tystnadsplikt. Advokatsamfundet anser inte att utredningen har redovisat och motiverat varför tystnadsplikten för dataskyddsombudet, såsom förslaget ser ut, endast ska omfatta uppgifter om enskilds personliga och ekonomiska förhållanden. I 8 kap. 4 § rättegångsbalken avgränsas en advokats tystnadsplikt med skrivningen att *”[e]n advokat är skyldig att förtiga vad han får kännedom om i sin yrkesutövning när god advokatsed kräver detta”.* För att inte personuppgiftsansvariga och personuppgiftsbiträden ska tveka att lämna all tänkbar och tillgänglig information till dataskyddsombudet i syfte att denne ska kunna utföra sina viktiga arbetsuppgifter, bör tystnadsplikten omfatta alla uppgifter som dataskyddsombudet erhåller i denna sin roll och inte endast uppgifter om enskilds personliga och ekonomiska förhållanden. En sådan sistnämnd begränsning leder också till svåra avväganden i fråga om vad som omfattas av dataskyddsombudets tystnadsplikt. En skrivning mer lik den i rättegångsbalken för advokater, bör gälla för dataskyddsombud inom såväl den privata som den offentliga sektorn.

Sekretess hos Datainspektionen

Advokatsamfundet anser att frågan om sekretess hos Datainspektionen bör ägnas uppmärksamhet i det fortsatta lagstiftningsarbetet. Den särskilda sekretessbestämmelsen i 32 kap. 1 § offentlighets- och sekretesslagen (2009:400) avser ärenden om tillstånd eller tillsyn som handläggs av Datainspektionen och omfattar sannolikt inte anmälan om personuppgiftsincidenter. Det finns en stor oro hos de personuppgiftsansvariga som ska anmäla personuppgiftsincidenter till tillsynsmyndigheten, eller som efter en konsekvensbedömning avseende dataskydd i vissa situationer är tvingade att begära förhandssamråd hos tillsynsmyndigheten, att uppgifter i dessa sammanhang, t.ex. känslig företagsinformation, inte kommer att kunna skyddas hos Datainspektionen. Blotta det faktum att ett företag har råkat ut för en personuppgiftsincident är information som kan vara mycket skadlig för ett företag, särskilt om företaget behandlar stora mängder information om privatpersoner eller behandlar känsliga personuppgifter.

Barns samtycke till behandling av personuppgifter

I 2 kap. 2 § regleras möjligheten för barn som har fyllt 13 år att lämna samtycke till behandling i samband med att informationssamhällets tjänster erbjuds direkt till barn. I betänkandet, på sidan 144, konstateras att ledning för tolkning av begreppet informationssamhällets tjänster kan hämtas i direktiv (EU) 2015/1535 respektive direktiv 2000/31/EG liksom i de tolkningar av begreppet som EU-domstolen har gjort. I betänkandet, på sidan

145, hänvisas därefter till EU-domstolens dom i mål nr C-291/13 (Papasavvas). Med tanke på att begreppet ”informationssamhällets tjänster” kan vara svårtolkat bör regeringen i lagrådsremissen närmare förtydliga, med hänvisning till EU-domstolens avgöranden, hur begreppet har tolkats. Ledning kan därvid sökas i EU-domstolens avgöranden i bl.a. C-236/08 till C-238/08 (Google France), C-324/09 (Ebay), C-108/09 (Ker-Optika), C-509/09 (EDate) och C-484/14 (McFadden).

Känsliga personuppgifter

I 3 kap. talas om känsliga personuppgifter. I artikel 9 i dataskyddsförordningen används begreppet särskilda kategorier av personuppgifter. Advokatsamfundet anser att dataskyddslagen rent principiellt bör använda samma begrepp som dataskyddsförordningen och inte skilja mellan känsliga personuppgifter och uppgifter om lagöverträdelse. Därutöver anser Advokatsamfundet att begreppet särskilda kategorier av personuppgifter för att utpeka vissa generellt sett skyddsvärda personuppgifter, är ett bättre begrepp än känsliga personuppgifter om man vill undvika begreppsförvirring. Det är nämligen så att även andra kategorier av personuppgifter än de som utpekas i 3 kap. i sitt sammanhang kan vara känsliga personuppgifter. Sålunda kan känsliga personuppgifter avse såväl dessa i 3 kap. särskilt utpekade personuppgifterna som andra typer av personuppgifter. Denna begreppsförvirring undviks om dataskyddslagen använder begreppet särskilda kategorier av personuppgifter.

E-förvaltningsområdet

Dataskyddsutredningen synes inte fullt ut ha berört den snabba utveckling som skett på e-förvaltningsområdet. När myndigheter enligt dataskyddsförordningen inte längre får behandla uppgifter med stöd av en intresseavvägning, och behandlingar med stöd av den registrerades samtycke inskränks, uppkommer osäkerhet om hur verksamheten ska kunna fortsätta utan ny omfattande särreglering. Som exempel kan nämnas s.k. eget utrymme (se prop. 2016/17:198), som endast innehavaren – inte myndigheten – ska ha tillgång till, men där *myndigheten* anses vara personuppgiftsansvarig för behandlingarna. Frågan blir om behandlingarna, enligt artikel 6.1 första stycket e) dataskyddsförordningen, kan vara nödvändiga för att utföra en uppgift av allmänt intresse. Denna grund för behandlingen måste emellertid enligt artikel 6.3 första stycket dataskyddsförordningen vara fastställd i enlighet med svensk rätt och enligt skäl 41 till förordningen bör denna grund vara tydlig och precis. Här behövs ett klargörande för att resultatet inte ska bli ett stort antal framställningar till regeringen om förordningsändringar för att varje myndighet ska kunna veta att behandlingen är laglig.

En möjlig tolkning av vad som utgör ett allmänt intresse kan vara att ansluta till de bedömningar som gjorts i regeringens proposition 2016/17:180, En modern och rättssäker förvaltning – ny förvaltningslag. Regeringen har där uttalat att kravet enligt den nya förvaltningslagen på legalitet – i likhet med 1 kap. 1 § regeringsformen – bör innebära ett krav på att myndighetens agerande ska ha stöd i någon av de källor som tillsammans bildar rättsordningen i vidsträckt mening. Kravet på legalitet ska enligt regeringen inte

heller uppfattas så att en myndighets åtgärd måste ha uttryckligt stöd i en viss lagbestämmelse eller i andra föreskrifter som har meddelats i enlighet med 8 kap. regeringsformen.

Dataskyddsutredningen har vidare i 3 kap. 3 §, beträffande myndigheters behandling, föreslagit en bestämmelse om att känsliga personuppgifter, med stöd av artikel 9.2 g) i dataskyddsförordningen, får behandlas under vissa förutsättningar. Detta författningsförslag torde dock exkludera den service som i dag ges genom eget utrymme, där myndigheten anses vara personuppgiftsansvarig. Lagförslagets tillämpningsområde är avgränsat till uppgifter som har lämnats i ett ärende eller till myndigheten. Uppgifter som finns i eget utrymme anses inte inkomna till myndigheten i förvaltningsrättslig eller tryckfrihetsrättslig mening och inte heller tillförda ett ärende (jfr prop. 2016/17:198). Eftersom myndigheten inte ska få ta del av innehållet i eget utrymme, kan myndigheten inte veta om känsliga uppgifter skrivs där i strid mot villkor för att få använda utrymmet. Liknande frågor aktualiseras i anknytning till myndigheternas numera långtgående säkerhetsarbete, där brandväggar, intrångsdetekteringssystem och spamfilter m.m. utgör en viktig del. Vid attacker och andra missbruk vet en myndighet inte och kan inte heller påverka vilka uppgifter som ”förs in” i dess it-miljö. Den föreslagna bestämmelsens tillämpningsområde bör utvidgas till att avse även dessa fall. På ett område synes redovisade frågor också ha beaktats genom ett särskilt undantag för förvaltning av vissa *system*, men då endast system avseende förvaltning av social omsorg, hälso- och sjukvårdstjänster (3 kap. 5 §). Motsvarande system används emellertid på andra områden där liknande behov finns av behandlingar, bl.a. för service- och säkerhetsändamål.

På liknande sätt bör den föreslagna generella sökbegränsningen i 3 kap. 4 § anpassas till den service som myndigheter ger åt privatpersoner. Här behövs en närmare avvägning mellan persondataskyddet och rätten till privatliv enligt den Europeiska konventionen om skydd för de mänskliga rättigheterna.

En behandling kan i vissa fall anses nödvändig med stöd av flera rättsliga grunder, t.ex. av både allmänt intresse och för att fullgöra ett avtal. I ett sådant fall aktualiseras emellertid även andra krav på funktioner såsom dataportabilitet (artikel 20 i dataskyddsförordningen). Det bör därför klargöras om en personuppgiftsansvarig som t.ex. tillhandahåller eget utrymme kan åberopa att behandlingarna är undantagna från rätten till dataportabilitet, eftersom ett allmänt intresse föreligger eller om det så snart ett avtal föreligger, t.ex. om eget utrymme, också finns en skyldighet att tillhandahålla funktioner enligt artikel 20, som rör dataportabilitet.

Personuppgifter som rör lagöverträdelser

I 3 kap. 9 § anges att *”[p]ersonuppgifter som rör fällande domar i brottmål, lagöverträdelser som innefattar brott eller straffprocessuella tvångsmedel får enligt artikel 10 i dataskyddsförordningen behandlas av myndigheter”*. Vidare framgår av 3 kap. 10 § att ”*[d]en myndighet som regeringen bestämmer får i enskilda fall besluta att andra än myndigheter får behandla sådana uppgifter som avses i 9 §”*. I utredningens författningskommentar på sidan 371 anges att *”[i] avvaktan på klargörande EU-rättslig*

praxis omfattas därför även fortsättningsvis uppgifter om misstankar om brott i viss utsträckning."

Den franska Högsta förvaltningsdomstolen, Conseil d'État, har den 15 maj 2017 i mål nr C-136/17 begärt förhandsbesked från EU-domstolen i ett antal frågor som rör sökmotorleverantörers skyldighet att ta bort länkar i sökresultat som är resultatet av en sökning på en privatpersons namn. Fråga 4, fjärde underfrågan, rör just begreppen lagöverträdelser och brottmålsdomar i artikel 8(5) i dataskyddsdirektivet (direktiv 95/46/EG):

"Ska bestämmelserna i artikel 8.5 i direktiv 95/46 tolkas så, att uppgifter om förundersökning avseende en person eller om en rättsprocess, och den efterföljande domen, utgör uppgifter om lagöverträdelser och brottmålsdomar? När en webbplats innehåller uppgifter om fällande domar och rättsliga förfaranden avseende en fysisk person omfattas den generellt av tillämpningsområdet för dessa bestämmelser?"

Artikel 10 i dataskyddsförordningen har ett snävare tillämpningsområde än artikel 8(5) dataskyddsdirektivet, eftersom dataskyddsförordningen endast omfattar uppgifter som "rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder" och inte "uppgifter om lagöverträdelser, brottmålsdomar eller säkerhetsåtgärder" som följer av dataskyddsdirektivet.

Redan artikel 8(5) har med stor sannolikhet inte avsetts få det vida tillämpningsområde som Högsta förvaltningsdomstolen i HFD 2016 ref. 8 givit bestämmelsen, eftersom begreppet "lagöverträdelser" i direktivet är snävare än misstankar om brott (denna fråga kommer sannolikt besvaras av EU-domstolen i mål nr C-136/17). När nu artikel 10 dataskyddsförordningen preciseras så att den endast avser "fällande domar i brottmål" är det olyckligt att utredningen föreslår en lydelse i 3 kap. 9 § som mer liknar 21 § personuppgiftslagen (1998:204) än artikel 10 i dataskyddsförordningen.

Överklagande av beslut som fattats av en myndighet i egenskap av personuppgiftsansvarig

I 8 kap. 2 § regleras rätten att överklaga vissa myndighetsbeslut rörande de registrerades rättigheter. Advokatsamfundet ställer sig frågande till varför rätten till dataportabilitet enligt artikel 20 inte omfattas av uppräkningen av beslut som ska kunna överklagas. Det finns heller ingen motivering därtill i betänkandet. Oaktat att rätten till dataportabilitet sällan kommer aktualiseras visavi myndigheter saknas anledning att inte låta jämväl dessa beslut vara överklagbara.

SVERIGES ADVOKATSAMFUND

Anne Ramberg