

Regeringskansliet
Infrastrukturdepartementet

Genomförande av direktivet om inrättande av en kodex för elektronisk kommunikation

Datainspektionen har granskat promemorian huvudsakligen utifrån myndighetens uppgift att arbeta för att människors grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter.

Med anledning av promemorians omfång och det antal frågor som behandlats har Datainspektionen valt att begränsa sitt yttrande till mer övergripande frågor och frågor av väsentlig betydelse för enskildas personliga integritet.

Utgångspunkt - tillämpliga europarättsliga bestämmelser

I promemorian lämnas förslag om att bestämmelser om säkerhet i nät och tjänster samt om integritetsskydd, i 6 kap. 3, 4, 4 a och 4 b §§ lagen 2003:389 om elektronisk kommunikation (LEK), upphävs. Dessa bestämmelser ersätts inte av några motsvarande bestämmelser i förslaget till ny lag om elektronisk kommunikation, i denna text benämnd LEK II. I avsnitt 18.1 i promemorian förs resonemang om att artiklarna 40 och 41 i direktiv 2018/1972 om inrättande av en europeisk kodex för elektronisk kommunikation (kodexdirektivet) ersätter såväl artiklarna 13a och 13b i ramdirektivet som artikel 4 i e-dataskyddsdirektivet, och att kommissionens förslag till ny e-dataskyddsförordning inte innehåller någon motsvarighet till artikel 4 i e-dataskyddsdirektivet. I avsnitt 18.4 i promemorian påpekas det dock att om det visar sig att e-dataskyddsförordningen inte antas kommer e-dataskyddsdirektivet fortsatt att gälla, vilket medför att det kan bli nödvändigt att vidta ytterligare åtgärder för att säkerställa att reglerna i artikel 4 i e-dataskyddsdirektivet fortsatt kan tillämpas i Sverige.

Medlemsstaterna ska senast den 21 december 2020 anta och offentliggöra de lagar och andra författningar som är nödvändiga för att genomföra

kodexdirektivet. Datainspektionen vill med hänsyn till detta påpeka att det är oklart huruvida den nya e-dataskyddsförordningen hinner beslutas och därefter bli tillämplig innan kodexdirektivet ska vara genomfört i nationell rätt. Utgångspunkten i det fortsatta lagstiftningsarbetet bör därför, enligt Datainspektionens mening, vara att e-dataskyddsdirektivet fortfarande gäller i sin helhet. Det krävs därför att de bestämmelser i LEK, som genomför e-dataskyddsdirektivet förs över till de nu föreslagna bestämmelserna.

Den föreslagna lagens tillämpningsområde

Genom det aktuella lagförslaget ändras definitionen av en *allmänt tillgängliga kommunikationstjänst* till att även omfatta s.k. interpersonella kommunikationstjänster (jfr 1 kap. 6 § LEK II). Ändringen innebär att personuppgiftsbehandling som idag faller under dataskyddsförordningen (GDPR), för vilken Datainspektionen är tillsynsmyndighet, kan komma att omfattas av LEK II och Post- och telestyrelsens (PTS) tillsynsområde. Det skulle i sig kunna innebära en omfattande förändring av de registrerades rättigheter, de personuppgiftsansvarigas skyldigheter vad gäller exempelvis IT-säkerhet samt vilka tillsyns- och sanktionsbefogenheter som är aktuella i olika situationer. De gränsdragningsfrågor som den föreslagna förändringen ger upphov till berörs dock inte i promemorian. I detta sammanhang hänvisar Datainspektionen till Europeiska dataskyddsstyrelsens uttalande angående samspelet mellan e-dataskyddsdirektivet och GDPR: https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_epri_vacydir_gdpr_interplay_en_o.pdf

Datainspektionen har i detta yttrande valt att lämna synpunkter vad gäller några specifika bestämmelser i förslaget. Datainspektionen efterlyser utöver detta dock även en övergripande analys av vad definitionsförändringen av allmänt tillgängliga kommunikationstjänster innebär vad gäller gränsdragningen mellan LEK II och GDPR.

Incidentrapportering

I förslaget har flera bestämmelser om incidentrapportering ersatt de bestämmelser som finns i 6 kap. 4, 4 a och 4 b LEK. Det är viktigt att den enskilda tillhandahållaren av en elektronisk kommunikationstjänst kan förstå vilken myndighet som är rätt mottagare av en incidentanmälan. Enligt nuvarande bestämmelse i 6 kap. 4 a § LEK gäller att tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster ska anmäla integritetsincidenter till PTS. Abonnenter och användare ska, enligt samma paragraf, informeras om incidenten om den kan antas påverka dem negativt. Enligt artikel 33.1 i GDPR ska en personuppgiftsincident anmälas till dataskyddsmyndigheten, såvida det inte är osannolikt att

personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Likaså ska information lämnas till de personuppgifterna berör om incidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Det har under nuvarande reglering, i 6 kap. 4 a § LEK, bedömts att tröskeln för att en incident ska anmälas är lägre än när en sådan krävs enligt GDPR, då en anmälan enligt LEK inte kräver att någon möjligen kan ha påverkats menligt av incidenten. Det har också bedömts att en anmälan till PTS inte leder till att registrerade skulle få sämre rättigheter vad gäller den information de får del av. Det har därigenom normalt bedömts att incidenter som inträffat vid tillhandahållandet av en elektronisk kommunikationstjänst ska anmälas till PTS.

Enligt de föreslagna bestämmelserna ska säkerhetsincidenter rapporteras till PTS om de haft en betydande påverkan på nät och tjänster. Tillägget om att påverkan ska vara "betydande" tyder på att det är en höjning av den tröskel som gäller för att en incidentanmälan ska göras till PTS. Informationen ska vidare lämnas till användaren eller abonnenten om det finns ett särskilt och betydande hot, vilket också är en höjning av den nivå som krävs för att information ska lämnas. Vidare har avgränsningen av vad som är en anmälningspliktig incident enligt det nu föreslagna regelverket förändrats, på grund av definitionsändringen av vad som är en elektronisk kommunikationstjänst (jfr 1 kap. 6 § LEK II). Eftersom det inte ska föreligga dubbla förpliktelser enligt regleringen om elektronisk kommunikation och GDPR, ska aktörer normalt inte behöva skicka en incidentanmälan både till Datainspektionen och till PTS för samma incident (jfr artikel 95 GDPR). Det är därför viktigt att det under lagstiftningsarbetet klargörs vad regeländringarna innebär gällande vilka incidenter som ska anmälas enligt LEK II, så att det finns en tydlig gränsdragning mot den skyldighet som gäller enligt artikel 33 i GDPR.

Eftersom de nu föreslagna bestämmelserna helt ersätter de gamla bör det under lagstiftningsarbetet också utvecklas hur det nya förslaget förhåller sig till artikel 4 i e-dataskyddsdirektivet såväl som till artikel 2 i kommissionens förordning (EU) nr 611/2013 om rapportering av personuppgiftsbrott (se resonemanget ovan angående tillämpliga europarättsliga bestämmelser).

Samverkan och samarbete

I promemorian föreslås att den närmare omfattningen av och formerna för samråd och samarbete mellan PTS och bl.a. Datainspektionen bör regleras i en förordning (jfr s. 327 i promemorian). Om en sådan reglering tas fram bör det beaktas att dataskyddsmyndigheten ska vara fullständigt oberoende i

utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med artikel 52.1 GDPR.

Övrigt

I promemorian föreslås att bestämmelserna om integritetsskydd och lagring av trafikuppgifter m.m. för brottsbekämpande ändamål förs över till den nya lagen (jfr s. 2 i promemorian). Av fotnoten på s. 49 framgår att förslaget motsvarar paragrafens lydelse enligt prop. 2018/19:86. Datainspektionen utgår därmed från att ingen ändring i sak är avsedd i förhållande till nuvarande reglering.

Detta beslut har fattats av enhetschefen Catharina Fernquist efter föredragning av juristen Mattias Sandström. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom och juristen Jennie Grön medverkat.

Catharina Fernquist, 2019-12-06 (Det här är en elektronisk signatur)