Datainspektionen informerar

Nr 1/2017

Allmänna råd

Datainspektionen har utarbetat en allmän vägledning för **integritetsanalys.**

Vägledningen ska tjäna som verktyg för att bedöma integritetsriskerna med ny eller ändrad lagstiftning.

Förhoppningen är att vägledningen bidrar till att myndigheterna tar fram integritetsanalyser och redovisar dem i sina betänkanden. Det i sin tur kan leda till lagförslag som bättre tar hänsyn till rätten till privatlivet som ju är en grundläggande rättighet.

Datainspektionen

den 10 maj 2017

Datainspektionen • Elverksgatan 10, AX-22100 Mariehamn, Åland • Besöksadress: Kvarteret iTiden
+358 (0)18 25 550 • +358 (0)457 34 320 81 • inspektion@di.ax • www.di.ax

Innehållsförteckning

1 Inledning

1.1 Syftet med vägledningen

Var och en har rätt till skydd för sitt privatliv och skydd av de personuppgifter som rör honom eller henne. Det följer av Europarättskonventionen, Europarådets dataskyddskonvention, EU:s stadga om de grundläggande rättigheterna, dataskyddsdirektivet och grundlagen. Det följer också av EU:s dataskyddsförordning som antogs den 14 april 2016 och som ska börja tillämpas den 25 maj 2018. Varje utredning måste därför reflektera över om föreslagen lagstiftning innebär någon form av personuppgiftsbehandling och i så fall göra en bedömning av det rättsliga stödet för personuppgiftsbehandlingen och de integritetsrisker som följer av förslagen.

Syftet med vägledningen är att underlätta arbetet med att analysera konsekvenserna för den personliga integriteten vid personuppgifts-behandling (integritetsanalys) när förslag till nya lagar eller beslutsunderlag tas fram.

I vägledningen redogörs för ett antal viktiga faktorer som behöver belysas i en integritetsanalys. Den utgör inget komplett verktyg utan behöver kompletteras med fördjupade analyser i det enskilda fallet.

En väl genomförd integritetsanalys ska utifrån ett bra beslutsunderlag svara på frågan om förslaget är förenligt med reglerna om skydd för den personliga integriteten i grundlagen och EU-rätten. Den ska också särskilt svara på frågan om konsekvenserna för den personliga integriteten som en föreslagen personuppgiftsbehandling medför, är proportionerliga i förhållande till det man avser att uppnå med behandlingen. I detta ingår att bedöma om behandlingen av personuppgifter är nödvändig utifrån de avsedda ändamålen med behandlingen och om det finns alternativ som är mindre integritetskänsliga. En förutsättning för en sådan analys är en noggrann kartläggning och beskrivning av den föreslagna personuppgiftsbehandlingen och en analys av vilka konsekvenser för den personliga integriteten behandlingen medför eller kan medföra.

2 EU:s dataskyddsförordning

EU:s dataskyddsförordning börjar tillämpas från och med den 25 maj 2018. Den kommer att ersätta dataskyddsdirektivet från 1995 och landskapslagen om behandling av personuppgifter inom landskaps- och kommunalförvaltningen. Förordningsformen innebär att bestämmelserna inte får ersättas med nationella bestämmelser, förutom i de fall förordningen ger uttryckligt stöd för det. Vid lagstiftningsarbete måste således utredas om författningsförslagen står i överensstämmelse med förordningens bestämmelser. Detta gäller även befintliga lagar. Konsekvensbedömningen i artikel 35 förordningen kan genomföras som ett led i lagstiftningsarbetet. Om detta har gjorts är den personuppgiftsansvariga befriad från kravet att genomföra en konsekvensbedömning innan behandling påbörjas[1]. Konsekvensbedömningen i lagstiftningsarbetet ska göras på ett sätt som uppfyller förordningens krav[2].

Dataskyddsförordningen innehåller många bestämmelser som är hämtade från dataskyddsdirektivet men även flera ändringar och nyheter såsom rätten att bli glömd, dataportabilitet, skyldighet att anmäla personuppgiftsincidenter och skyldighet för den personuppgiftsansvariga att göra en konsekvensbedömning avseende dataskydd innan en riskfylld behandling kan påbörjas.

Denna vägledning kan användas som ett hjälpmedel vid genomförandet av konsekvensanalysen.

3 Checklista

Tänk redan från början på vilka konsekvenser som utredningens uppdrag och tänkbara förslag kan komma att få för skyddet för den personliga integriteten i samband med behandling av personuppgifter.

3.1 Kartläggning

- Vilket behov av att behandla personuppgifter hos myndigheter och organisationer kan uppkomma med anledning av utredningens uppdrag och förslag?
- För vilka ändamål ska personuppgifter behandlas?

[1] Dataskyddsförordningen artikel 35.10

[2] WP29-dataskyddsarbetsgruppen har nyligen på sin hemsida http://ec.europa.eu/justice/data-protection/index_en.htm publicerat ett utkast till handbok som preciserar när och hur en konsekvensanalys ska genomföras. Handboken är på engelska men den kommer också att översättas till svenska.

- Med vilket rättsligt stöd ska personuppgifterna behandlas?
- Vem ska utför personuppgiftsbehandlingen och vem svarar för den?
- Vilka personuppgifter kommer att behöva samlas in och i övrigt behandlas?
- Hur många personer kommer att beröras av personuppgiftsbehandlingen och hur många uppgifter om varje person kommer att behöva samlas in?
- Varifrån ska personuppgifterna samlas in?
- Vilka kommer att ha åtkomst till personuppgifterna och vilken spridning kan uppgifterna i övrigt komma att få?
- Finns det behov av nya sekretessbestämmelser?
- Vilka sök- och sammanställningsmöjligheter är nödvändiga för ändamålet och hur kan de begränsas?
- Hur länge behöver personuppgifter bevaras?
- Vilket inflytande kommer de registrerade att ha över personuppgiftsbehandlingen?
- Vilken information om behandlingen av personuppgifter kommer de registrerade att få?
- Vilka (befintliga eller nya) bestämmelser kommer att gälla som skydd för de registrerades personliga integritet vid den föreslagna personuppgiftsbehandlingen?

3.2 Analys och proportionalitetsbedömning

- Finns det några mindre integritetsingripande alternativ för att uppnå det avsedda ändamålet än den föreslagna personuppgiftsbehandlingen?
- Hur förbehåller sig förslaget gällande rätten till skydd för privatlivet och rätten till skydd för personuppgifter enligt grundlagen, Europakonventionen och EU:s rättighetsstadga?
- Vad regleras i dataskyddsförordningen och vad får respektive lagstiftande organ reglera i nationell rätt?
- Innebär förslaget sådana integritetsrisker att det krävs särskild reglering i lag?
- Står integritetsintrånget som behandlingen medför i rimlig proportion till den nytta som behandlingen innebär för de avsedda ändamålen?