Datainspektionen informerar

Nr 2/2018

Allmänna råd

Datainspektionen ger ut allmänna råd i syfte:

- att öka personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om sina skyldigheter enligt EU:s dataskydds-förordning samt
- att öka allmänhetens medvetenhet om och förståelse för risker, regler, skyddsåtgärder och rättigheter i fråga om behandling av personuppgifter.

De allmänna råden är inte bindande, utan innehåller riktlinjer om hur de bindande kraven i dataskyddsförordningens kan uppnås. Detta dokument behandlar **personuppgiftsansvar.**

Datainspektionen

den 9 april 2018

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

Innehåll

1 Personuppgiftsansvar

En myndighet som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter är personuppgiftsansvarig i enlighet med artikel 4.7 i EU:s dataskyddsförordning[1], som träder i kraft den 25 maj 2018.

Personuppgiftsansvarig är således den juridiska person (en myndighet) som behandlar personuppgifter i sin verksamhet och som bestämmer vilka uppgifter som ska behandlas och vad de ska användas till. Det är alltså inte chefen på en arbetsplats eller en anställd som formellt är personuppgiftsansvarig, även om myndighetens tjänstemän naturligtvis har ett tjänsteansvar beträffande sina handlingar och underlåtelser.

Det är de faktiska omständigheterna i det enskilda fallet som avgör vilken myndighet som är personuppgiftsansvarig. Om två eller flera myndigheter gemensamt bestämmer över en viss behandling är de personuppgiftsansvariga tillsammans. Ansvarig myndighet kan också anges i lagstiftning, till exempel i särskilda registerlagar.

En användare som enbart har rätt att komma åt personuppgifter genom att läsa dem och söka bland dem men som inte självständigt får ändra, komplettera eller radera uppgifterna är inte personuppgiftsansvarig.

En myndighet är personuppgiftsansvarig även om verksamheten bedrivs i andra organisatoriska enheter inom myndigheten. Om flera myndigheter/juridiska personer inom en och samma organisation (en kommun eller Ålands landskapsregering) behöver behandla samma personuppgifter kan ansvarsfördelningen se ut på olika sätt:

- Om kommunen eller Ålands landskapsregering på egen hand bestämmer över behandlingen blir kommunen eller Ålands landskapsregering personuppgiftsansvarig.

- Om alla myndigheter inom kommunen eller Ålands landskapsregering gemensamt bestämmer över behandlingen blir de tillsammans ansvariga för det aktuella registret. Över andra register som de självständigt bestämmer över är de självständigt personuppgiftsansvariga för.

Det avgörande vid bestämmande av personuppgiftsansvarig är myndigheten som sådan oberoende av om den är uppdelad i avdelningar, enheter eller byråer. Huvudregeln är att myndigheten anses personuppgiftsansvarig för de behandlingar den beordrar. Undantag kan möjliggöras genom att en annan ordning skapas i en särskild lagstiftning. Om myndigheten erbjuder registeruppgifter via t.ex. en databas med personuppgifter med hjälp av en teknisk

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

förbindelse är det myndigheten som är ansvarig för utomståendes behandling och sökning i systemen. Om däremot den utomstående vidtar vidare bearbetning i insamlade material överförs ansvaret över på den som bearbetat materialet[1]. I kommunerna är i regel både kommunstyrelsen och de kommunala nämnderna – om de är så självständiga att de är förvaltningsmyndigheter - personuppgiftsansvariga, var och en i sin verksamhet. Vilket organ i kommunen som är ansvarigt för personuppgifter kan variera; de faktiska omständigheterna måste prövas i varje enskilt fall, till exempel om nämnden självständigt förfogar över de personuppgifter som behandlas.

Om myndigheten anlitar en utomstående systemleverantör som även sköter driften och lagrar myndigheternas personuppgifter i sina datorer, krävs att myndigheten ingår avtal med leverantören. I avtalet ska regleras hur personuppgifterna får hanteras och hur ansvaret och förpliktelserna i samband med registreringen hanteras. T.ex. får leverantören behandla personuppgifterna bara i enlighet med instruktioner från myndigheten och leverantören är skyldig att vidta åtgärder för att upprätthålla god IT-säkerhet.

I avtal om köptjänster definieras vilka rättigheter och skyldigheter myndigheten och den privata serviceproducenten har. När avtal om köptjänster ingås är det skäl att i avtalen ta in bestämmelser om hur handlingarna ska förvaltas, hur de ska göras upp, bevaras, utplånas eller arkiveras. Det är dessutom skäl att i avtalet reglera hur upplysningar om handlingarna ska ges till den registrerade eller till en person i partsställning eller någon annan utomstående.

Vid publicering på Internet har myndigheter ett ansvar för vad de publicerar. Om en myndighet har möjlighet att bestämma över ändamål och medel för en publicering gjord av andra besökare än organisationen är den ansvarig även för denna publicering. Myndighetens ansvar utesluter inte att även besökarna är ansvariga för det de publicerar.

2 Krav på register över behandling av personuppgifter

Enligt artikel 30.1 i dataskyddsförordningen är personuppgiftsansvarig myndighet skyldig att föra ett register över behandling av personuppgifter som har utförts under dess ansvar. Registret ska innehålla:

a) namn och kontaktuppgifter för den personuppgiftsansvarige, samt i tillämpliga fall gemensamt personuppgiftsansvariga, den personuppgiftsansvariges företrädare samt dataskyddsombudet,

b) ändamålen med behandlingen av personuppgifterna,

[1] Ålands landskapsregerings framställning FR 8/2003-2004

c) en beskrivning av kategorierna av registrerade personer och av kategorierna av personuppgifter,

d) kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, inbegripet mottagare i tredjeländer eller i internationella organisationer,

e) i tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation,

f) de förutsedda tidsfristerna (om möjligt) för radering av de olika kategorierna av uppgifter,

g) en allmän beskrivning (om möjligt) av tekniska och organisatoriska säkerhetsåtgärder som vidtagits för att säkerställa en lämplig säkerhetsnivå med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter.

Exempel på nättjänster, som kan behöva beskrivas i ett register, är diskussionsfora som förutsätter registrering eller insamling av information genom internet (kundförfrågningar, anmälningsblanketter och insamling av besökarrespons m.m.).

I artikel 30.5 finns ett undantag från skyldigheten att upprätta registerbeskrivningar för företag eller organisationer som sysselsätter färre än 250 personer. Dock gäller detta undantag inte all behandling av personuppgifter. Även om antalet anställda är mindre än 250 personer **måste** register över behandling ändå föras ifall något av följande gäller:

- Behandlingen kommer sannolikt att medföra en risk för registrerades rättigheter och friheter (exempel: lokalisering av anställda genom GPS),
- Behandlingen är inte tillfällig (exempel: behandling av anställdas personuppgifter för att kunna betala ut löner, eller
- Behandlingen omfattar särskilda kategorier av personuppgifter enligt artikel 9 eller personuppgifter som rör fällande domar i brottmål samt överträdelser enligt artikel 10 (exempel: behandling av uppgifter om anställdas hälsa).

Eftersom de allra flesta företag eller organisationer betalar lön **regelbundet** till sina anställda omfattas de också av skyldigheten att upprätta register över åtminstone denna behandling. Däremot behöver andra sorters behandling inte tas med i registret ifall företaget eller organisationen har färre än 250 anställda.

Detta dokument ersätter Datainspektionen informerar Nr 5/2011, Registeransvar.