DIGG - Myndigheten för digital förvaltning

# Etablering av förvaltningsgemensam digital infrastruktur

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

Bolagsverket, Domstolsverket, E-hälsomyndigheten, Försäkringskassan, Lantmäteriet, DIGG, Myndigheten för samhällsskydd och beredskap, Riksarkivet och Skatteverket har fått i uppdrag av regeringen att tillsammans etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte (Infrastrukturen). Uppdraget redovisas i en slutrapport.

DIGG uppger i missivet att det finns bilagor till slutrapporten som myndigheten undanber synpunkter på eftersom det finns begränsad möjlighet att hantera dessa synpunkter innan inlämning av slutrapporten. Datainspektionen lämnar därför inte några synpunkter på dessa bilagor.

Datainspektionen lämnar följande synpunkter på slutrapporten.

Det är en informativ slutrapport med generella beskrivningar av säkerhetsskydd, informationssäkerhet och dataskydd. Datainspektionen ser positivt på att dataskyddsfrågor tagits upp i slutrapporten.

Utifrån beskrivningarna i rapporten konstaterar Datainspektionen att det verkar kvarstå mycket arbete med Infrastrukturen och att det kommer krävas noggranna rättsliga överväganden vad gäller skyddet för den personliga integriteten och informationssäkerhet, eftersom det kan komma att ske omfattande personuppgiftsbehandlingar i de olika delarna i Infrastrukturen.

Det kan tilläggas att även personuppgiftsbehandlingar som sker i framtida testverksamhet också omfattas av dataskyddsförordningen och kompletterande lagstiftning.

Datainspektionen välkomnar därför förslaget om att det bör tillsättas en statlig utredning som analyserar de rättsliga förutsättningarna för Infrastrukturen och utreder behovet av en sammanhållen lagstiftning inom området.

Många myndigheter föreslås ha olika ansvarsområden och roller i Infrastrukturen. Det är därför viktigt att personuppgiftsansvaret utreds för de olika aktörerna. Att personuppgiftsansvaret är utrett och klarlagt är avgörande för att den personuppgiftsansvariga ska uppfylla ansvarsskyldigheten i artikel 5.2 dataskyddsförordningen och för att dataskyddsregelverket ska efterlevas. Att reglera personuppgiftsansvar i författning kan vid komplexa behandlingar med flera aktörer vara ett bra alternativ, men då behövs även en ordentligt genomförd integritetsanalys, se nedan.

De grundläggande principerna i artikel 5 dataskyddsförordningen behöver också följas i Infrastrukturen, såsom exempelvis ändamålsbegränsning, uppgiftsminimering och principen om integritet och konfidentialitet.

Dataskyddsförordningen behöver även beaktas vid bedömningen av vilka säkerhetsåtgärder som är lämpliga för Infrastrukturen. Säkerhetsåtgärderna ska bedömas utifrån skyddet för den enskildes grundläggande fri- och rättigheter. I detta sammanhang behöver särskilt artiklarna 5.1 f, 25 och 32 dataskyddsförordningen beaktas. Att integrera nödvändiga skyddsåtgärder är ett sätt att säkerställa att kraven i dataskyddsförordningen uppfylls och att de registrerades rättigheter skyddas.

Om en statlig utredning tillsätts är det av största vikt att det görs en analys av hur förslagen förhåller sig till dataskyddsförordningen och att det görs en fullständig integritetsanalys. I integritetsanalysen ska de risker och konsekvenser förslagen kan innebära för den personliga integriteten kartläggas och behovet av skyddsåtgärder och alternativa lösningar bedömas. För att uppfylla kraven i ett konkret lagstiftningsärende måste behandlingen vara proportionell, vilket innebär att det intrång som sker i den enskildes privata sfär måste vara befogat och inte större än nödvändigt.

Datainspektionen hänvisar till Inspektionens *Vägledning för integritetsanalys* som syftar till att underlätta arbetet med att analysera konsekvenserna för den personliga integriteten vid personuppgiftsbehandling när förslag till författningar och föreskrifter tas fram. Vägledningen utarbetades innan dataskyddsförordningen började tillämpas, men innehåller hänvisningar till dataskyddsförordningen och grundlagsskyddet. Vägledningen bifogas.

Vid framtagande av nationell rätt finns även möjlighet att genomföra en konsekvensbedömning av föreslagna nationella bestämmelser enligt artikel 35.10 dataskyddsförordningen. Av bestämmelsen framgår följande:

*”Om behandling enligt artikel 6.1 c eller e har en rättslig grund i unionsrätten eller i en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av, reglerar den rätten den aktuella specifika behandlingsåtgärden eller serien av åtgärder i fråga och en konsekvensbedömning avseende dataskydd redan har genomförts som en del av en allmän konsekvensbedömning i samband med antagandet av denna rättsliga grund, ska punkterna 1–7 inte gälla, om inte medlemsstaterna anser det nödvändigt att utföra en sådan bedömning före behandlingen.”*

En konsekvensbedömning kan med fördel genomföras inom ramen för lagstiftningsarbetet så långt det är möjligt, trots att man på det stadiet inte har exempelvis de tekniska förutsättningarna och därmed kanske inte heller behovet av konkreta säkerhets- och skyddsåtgärder helt klart för sig. Det gör kommande tillämpning förutsägbar och ger även en grund för den konsekvensbedömning den personuppgiftsansvariga sedan kan behöva göra för att kunna minimera eventuella höga risker med kommande personuppgiftsbehandlingar.

---

Detta beslut har fattats av juristen Linn Sandmark. Vid den slutliga handläggningen har it-säkerhetsspecialisten Johan Ma medverkat.

*Linn Sandmark, 2020-12-14 (Det här är en elektronisk signatur)*