



E-förvaltning och personuppgiftslagen

Statliga myndigheters behandling av personuppgifter

När myndigheterna utvecklar e-tjänster och inför elektroniska ärendehanteringssystem innebär det en ökad datoriserad behandling av personuppgifter. Hanteringen av personuppgifter får inte kränka enskildas personliga integritet och myndigheterna måste därför se till att följa reglerna i personuppgiftslagen (PuL), särskild registerlagstiftning och offentlighets- och sekretesslagstiftningen. Det här dokumentet ger råd och vägledning för behandlingen av personuppgifter i samband med e-förvaltning.

Publicering av information på Internet

Diariet. Myndigheterna är enligt offentlighets- och sekretesslagen med vissa undantag skyldiga att diarieföra handlingar som kommer in till eller upprättas vid myndigheten. Ett diarium ska vara utformat så att det underlättar allmänhetens insyn och får innehålla de uppgifter som krävs för att det ska vara möjligt att identifiera allmänna handlingar. Som huvudregel gäller att diariet inte bör innehålla fler personuppgifter än de som anges i offentlighets- och sekretesslagen. Sådana uppgifter är diarienummer och, om uppgifterna inte är sekretessbelagda, uppgift om vem handlingen kommit från eller till vem den har expedierats samt uppgift om vad handlingen rör.

När en myndighet på eget initiativ tillgängliggör personuppgifter i diariet på Internet går den utöver sina skyldigheter enligt andra kapitlet Tryckfrihetsförordningen (TF). Det innebär att personuppgiftslagen gäller. Det kan då, beroende på myndighetens verksamhetsområde och på vad uppgifterna innehåller, bli fråga om att publicera endast ett begränsat urval av de uppgifter som ingår i diariet. Diariet bör till exempel inte innehålla personnummer, uppgifter om adresser och telefonnummer, känsliga personuppgifter enligt 13 § personuppgiftslagen eller personuppgifter om lagöverträdelser.



Allmänna handlingar. Personuppgifter får inte publiceras på Internet bara för att de ingår i en allmän handling och inte är sekretessreglerade. Även om uppgifter kan lämnas ut på någons begäran utan hinder av sekretess, måste myndigheten ta hänsyn till integritetsskyddsreglerna i personuppgiftslagen för att kunna publicera uppgifterna. Det innebär bland annat att det måste finnas ett berättigat ändamål, att publiceringen inte kränker den registrerades personliga integritet och att myndighetens intresse av att publicera uppgifterna måste väga tyngre än den enskildes intresse att skydda sin personliga integritet.

E-tjänster

Autentisering. För vissa e-tjänster kan det finnas behov av att verifiera identiteten hos användarna (autentisering). Valet av autentiseringsmetod bör utgå från känsligheten hos de personuppgifter som behandlas, mängden uppgifter och de risker som är förknippade med behandlingen.

E-tjänster där användarna kan ta del av personuppgifter som är känsliga enligt 13 § personuppgiftslagen eller andra uppgifter som annars är särskilt känsliga, som uppgifter om lagöverträdelse och uppgifter som är sekretessreglerade, kräver normalt mer avancerade metoder för autentisering, som exempelvis e-legitimation eller engångslösenord. E-tjänster av typen "Mina sidor" motiverar mer avancerade metoder för identifiering av användarna. Framför allt gäller detta om användaren efter inloggning kommer åt ett stort antal personuppgifter som inte kan hänföras till ovan angivna kategorier av uppgifter men som sammantaget kan vara integritetskänsliga.

Överföring av personuppgifter via Internet. När en myndighet erbjuder allmänheten e-tjänster på webben eller via e-post kan det inträffa att integritetskänslig information utväxlas mellan parterna. Personuppgifter som är känsliga enligt 13 § personuppgiftslagen eller andra uppgifter som annars är särskilt känsliga, som uppgifter om lagöverträdelse och uppgifter som är sekretessreglerade, måste krypteras när de överförs i öppna nätverk som exempelvis Internet. Användaren av e-tjänsten måste kunna förvissa sig om att det är myndigheten som är mottagare av uppgifterna. Detta kan myndigheten lösa genom att till exempel använda ett signerat servercertifikat och SSL/TLS. *

Information. Myndigheten är i regel skyldig att i anslutning till e-tjänsterna lämna information till användarna om behandlingen av personuppgifter. Det gäller oavsett om uppgifterna samlas in med eller utan de registrerades samtycke. Informationen ska upplysa om vem som är personuppgiftsansvarig, ändamålen med behandlingen, vilka som är mottagare av uppgifterna, eventuell skyldighet för den enskilde att lämna uppgifter och rätten att ansöka om registerutdrag och få felaktiga uppgifter rättade. Normalt kan informationen lämnas i en särskild ruta eller i ett särskilt fönster på webbplatsen i anslutning till e-tjänsten.

Dokument- och ärendehanteringssystem

"Internt diarium". Ibland används begreppet diarium även på register som används internt inom myndigheten som en innehållsförteckning för dokument- och ärendehanteringssystemet. Ett diarium som används för sådana ändamål – att sortera bland ärenden – ger ett något större utrymme att registrera personuppgifter. Sådana "diarier" kan bland annat innehålla personnummer, adresser, telefonnummer och

* SSL/TLS är säkra kommunikationsprotokoll som främst används för att krypteringsskydda kommunikation på webben. Det stödjer också autentisering av både server och användare genom användning av certifikat, som exempelvis servercertifikat och e-legitimationer.

uppgifter om ärendet, utöver den information som lämnas i ärenderubriken. Registreringen av uppgifter måste alltid vara motiverad utifrån ändamålet. *

Tillgången till uppgifter. Dokument- och ärendehanteringssystem kan innehålla stora mängder personrelaterad information. En grundläggande princip är att anställda inom en myndighet endast bör ha elektronisk tillgång till personuppgifter som de behöver för sitt arbete. Detta gäller även om uppgifterna är offentliga. Behovet av åtkomst varierar naturligtvis beroende på myndighetens verksamhetsområde och den anställdes arbetsuppgifter. För att begränsa den elektroniska tillgången ska myndigheten ha ett system för behörighetsstyrning. Obehörig åtkomst måste också begränsas genom fungerande rutiner, till exempel arbetsrutiner, rutiner för utbildning och information till anställda samt rutiner för logguppföljning.

Sökbegrepp. Vilka sökbegrepp myndigheten får använda framgår ofta av särskild registerlagstiftning. Om personuppgiftslagen är tillämplig måste varje sökning göras för ett berättigat ändamål som har sin grund i verksamheten. Det innebär att anställda inte får söka efter uppgifter i systemen av privata skäl. Myndigheten bör införa tekniska sökbegränsningar i dokument- och ärendehanteringssystemet som är anpassade för just de ändamål som personuppgifterna används till av myndigheten.

Arkivering. Även om en myndighet enligt arkivlagen har rätt att arkivera handlingar bör tillgången till handlingarna begränsas. Det är inte lämpligt att systemet gör det möjligt med obegränsade sökningar bland alla inskannade handlingar som någonsin kommit in till myndigheten. När myndigheten arkiverar handlingar bör de avskiljas från det diarium och dokument- och ärendehanteringssystem som används i den dagliga verksamheten. Om arkiveringsfunktionen ingår i samma system bör systemet innehålla tekniska avgränsningar.

Åtkomst till skyddade personuppgifter. För att obehöriga inte ska komma åt skyddade personuppgifter är det bland annat viktigt att det vid myndigheten finns sekretessmarkeringar som syns tydligt vid sökningar i register och att all personal som hanterar personuppgifter ges grundlig information om skyddade personuppgifter och sekretessfrågor. Kretsen av personer som har tillgång till skyddade personuppgifter måste begränsas så mycket som möjligt. Sådana personuppgifter får inte spridas till områden där sekretess för uppgifterna inte föreligger. Myndigheten bör regelbundet följa upp att regler och rutiner kring skyddade personuppgifter efterlevs och respekteras.

Teknisk och administrativ säkerhet

Myndigheter måste ha väl avvägda rutiner för behörighetstilldelning och tydliga riktlinjer för när det är tillåtet för personal att ta del av personuppgifter. För att kunna utreda felaktig eller obehörig användning av personuppgifter bör det dessutom finnas en logg som sparas viss tid och följs upp. Det är viktigt att göra klart för de anställda vad som är tillåtet, hur efterlevanden av dessa regler kontrolleras och vad som händer om man bryter mot reglerna. Myndigheten ska också tekniskt begränsa åtkomstmöjligheterna så mycket som det är faktiskt och praktiskt möjligt med hänsyn till den aktuella verksamheten och känsligheten hos personuppgifterna.

Det ska också finnas rutiner för registrering av personuppgifter i diarium, hantering av känsliga personuppgifter och brottsuppgifter samt gallring. Det är lämpligt att uppgifter som görs tillgängliga offentligt registreras centralt av personer med

* Även om det diarium som förs med stöd av offentlighets- och sekretesslagens bestämmelser och det "diarium" som används internt rent tekniskt inte utgör två separata register kan man för att underlätta en bedömning enligt personuppgiftslagen se de olika diarierna som två separata diarium med var sitt ändamål.

kunskaper om personuppgiftslagen, exempelvis registrator. När myndigheten erbjuder e-tjänster måste den ha tydliga och väl avvägda tekniska och administrativa rutiner för att kunna säkerställa identiteten hos användaren av en e-tjänst i de fall det är nödvändigt, skydda personuppgifter som förs över i öppna nät så att obehöriga inte kan ta del av dem samt skydda personuppgifter som samlats in.

Personuppgiftsansvar

En myndighet är personuppgiftsansvarig för den behandling av personuppgifter som sker inom den egna verksamheten. Det innebär att myndigheten normalt sett även är ansvarig för den behandling av personuppgifter som sker genom e-tjänster, som exempelvis när sådana e-tjänster som "mina sidor" erbjuder möjligheter för den enskilde att på myndighetens webbplats registrera uppgifter. Den personuppgiftsansvarige ansvarar för att personuppgiftslagen följs och att de registrerade behandlas korrekt.

Personuppgiftsansvarig är den eller de som tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. När olika myndigheter samarbetar och utåt uppträder som en gemensam enhet kan det uppstå oklarheter om personuppgiftsansvaret. Det är möjligt att överlåta den faktiska behandlingen av personuppgifter men personuppgiftsansvaret kan aldrig överlåtas. Däremot kan personuppgiftsansvaret delas av flera om de gemensamt samlar in och behandlar vissa personuppgifter. Myndigheterna måste ha klart för sig vilken myndighet som är personuppgiftsansvarig och detta ska också framgå utåt så att de registrerade kan ta tillvara sina rättigheter i samband med behandlingen.

Om en utomstående leverantör behandlar personuppgifter för en myndighets räkning, till exempel om de lagras på en server hos leverantören, blir denne ett personuppgiftsbiträde. Myndigheten måste då i egenskap av personuppgiftsansvarig upprätta ett skriftligt avtal – ett så kallat biträdesavtal – med leverantören. I avtalet ska det föreskrivas att leverantören får behandla personuppgifterna bara i enlighet med instruktioner från myndigheten och att leverantören är skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda uppgifterna.

Den personuppgiftsansvarige ska förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och även se till att personuppgiftsbiträdet verkligen vidtar åtgärderna.

Mer information

Mer information om vad som gäller för behandling av personuppgifter inom e-förvaltning finns bland annat i följande informationsmaterial som du hittar på Datainspektionens webbplats www.datainspektionen.se/ladda-ner

-  [Vägledning för kommuner: Personuppgifter och e-förvaltning](#)
-  [Säkerhet för personuppgifter, Datainspektionens allmänna råd](#)
-  [Information till registrerade enligt PuL, Datainspektionens allmänna råd](#)

Kontakta Datainspektionen

E-post: datainspektionen@datainspektionen.se Webb: www.datainspektionen.se
Tfn 08-657 61 00. Postadress: Datainspektionen, Box 8114, 104 20 Stockholm.



Datainspektionen