Datainspektionen informerar

Nr 4/2018

Allmänna Råd

Datainspektionen ger ut allmänna råd i syfte:

1) att öka personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om sina skyldigheter enligt EU:s dataskyddsförordning samt

2) 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 rekommendationer om hur de bindande kraven i dataskyddsförordningens kan uppnås. Detta dokument innehåller principer för inbyggt dataskydd (privacy by design) och är en **vägledning för hur IT-system bör utformas** för att redan från början uppfylla kraven i dataskyddsförordningen.

Datainspektionen

den 12 april 2018

di.ax datainspektionen

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. Inledning

Utveckling av tekniska system är komplicerade processer där hänsyn ska tas till många olika krav. Ett av kraven, som måste ställas, är värnande om människors personliga integritet. Det är nödvändigt att integritetsfrågor beaktas under ett IT- systems hela livscykel, från början till slut, så att systemet ska kunna hålla en hög säkerhetsnivå samt så att dataskyddsförordningen[1] ska kunna efterlevas. Genom att från första början vidta åtgärder för att efterleva dataskyddsförordningen undviker myndigheterna att systemen måste göras om. När integritetsfrågorna beaktas från början kan vi undvika att det uppstår tidsödande arbetsinsatser och ökade kostnader på grund av att bristande dataskydd måste åtgärdas i efterhand. Ett ofta använt begrepp är inbyggt dataskydd som innebär att dataskyddet påverkar systemets hela livscykel – från förstudie via design och utveckling till användning och avveckling.

2. Digital utveckling

Landskapsregeringen har i sin digitala agenda valt att prioritera organisations-övergripande service, gemensamma IT-stöd samt E-förvaltning med ålänningarnas behov i centrum. E-förvaltning definieras inom EU som ”verksamhetsutveckling i offentlig förvaltning som drar nytta av informations- och kommunikations-teknik kombinerad med organisatoriska förändringar och nya kompetenser”.

Användningen av informations- och kommunikationsteknik (IKT) i förvaltningen kommer i allt större utsträckning att underlätta ålänningarnas kontakter med skola, sjuk- och hälsovård samt annan offentlig verksamhet.

Det offentliga Åland håller nu på att förbereda för e-tjänster (elektroniska tjänster). Planen är att ålänningarna ska kunna få tillgång till alla offentliga tjänster på ett och samma ställe med bara en inloggning med hjälp av bankkoder, mobilcertifikat eller identitetskort. Det ska vara möjligt att betala exempelvis ansökan om hembygdsrätt, direkt via e-tjänsten. En annan förändring är en större närvaro i de sociala medierna.

Den tekniska utvecklingen har stora praktiska fördelar, men innebär en hel del utmaningar när det gäller integritetsskydd. Samtidigt som det blir lättare att lämna uppgifter om sig själv till myndigheterna och att erhålla uppgifter från myndigheterna, måste myndigheterna tänka mer på lösningar som skyddar personuppgifter från förvanskning eller obehörigt utlämnande eller förstörande.

[1] Härmed avses 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.

3. Personuppgiftsansvar

En myndighet är personuppgiftsansvarig[2] för den behandling av personuppgifter som sker inom den egna verksamheten. Det innebär att myndigheten i regel också är ansvarig för den behandling av personuppgifter som sker genom e-tjänster. Det kan t.ex. gälla behandling av uppgifter som lämnas till myndigheten eller när sådana e-tjänster som ”Mina sidor” erbjuder möjlighet att på myndighetens hemsida registrera uppgifter. Således ska den personuppgiftsansvariga myndigheten se till att upprätthålla ett gott skydd för de personuppgifter som behandlas i verksamheten.

Till de viktigaste skyldigheterna för en personuppgiftsansvarig myndighet hör inbyggt dataskydd och dataskydd som standard. I artikel 25.1 i dataskyddsförordningen föreskrivs att med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder vilka ska vara utformade för ett effektivt genomförande av dataskyddsprinciper och för integrering av de nödvändiga skyddsåtgärderna i behandlingen. Vidare föreskrivs det i artikel 25.2 att den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Det preciseras i artikel 25.2 att skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet och att dessa åtgärder framför allt ska säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer

Eftersom IT-stödet som används inte får medföra integritetsrisker, måste tydliga krav formuleras till leverantören av IT-stödet. Även om en leverantör av IT-produkter i allmänhet inte är ansvarig för de eventuella integritetsproblem som uppstår i samband med användningen av produkten är det viktigt att den har de nödvändiga funktionerna för integritetsskydd. Också i det fall det istället för hårdvara eller programvara är fråga om en tjänst som levereras genom outsourcing eller molntjänster. Beställaren, måste för att uppfylla sitt personuppgiftsansvar ansvarig, se till att leverantören uppfyller kraven på säkerhet och integritetsskydd.

I de fall myndigheten har lagt ut databehandlingen på ett personuppgiftsbiträde ska det finnas ett avtal som reglerar hur personuppgiftsbiträdet ska behandla uppgifterna och vilka säkerhetsåtgärder som ska vidtas. Se närmare om det i Datainspektionens allmänna råd angående personuppgiftsbiträdens behandling av personuppgifter för personuppgiftsansvariga myndigheters räkning.

[2] Personuppgiftsansvarig är, enligt artikel 4.7 i dataskyddsförordningen, den myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter

4. Checklista för IT-projekt

Dataskyddet förutsätter en strukturerad arbetsmetod som är jämförbar med kvalitetssäkring. Det behövs en riskanalys där konsekvenserna för de registrerade individernas integritet kartläggs. Följande kan vara bra att tänka på:

4.1. Begränsning av mängden personuppgifter

IT-system ska vara utformade så att så få personuppgifter som möjligt samlas in och behandlas. Därför är det viktigt att bestämma vilka personuppgifter som verkligen behövs för att tillgodose ändamålet. Det gäller såväl när krav ställs och i samband med systemets formgivning som i skedet när uppgifterna samlas in. Ändamålet för behandlingen är avgörande för vilka krav som ska ställas på systemet. Det är därför viktigt att ändamålet för behandlingen är bestämt i förväg.

Integritetsriskerna kan begränsas t.ex. genom att:

- uppgifterna ändras så att de blir mindre känsliga,
- uppgifterna begränsas till att endast indirekt peka ut en individ,
- namn ersätts med pseudonymer,
- det undviks att personbeteckning rutinmässigt tas med som fält i databaser.

Om ett ärendehanteringssystem i sig kan göra mer med personuppgifter än vad som behövs för ändamålet, ska de funktionerna begränsas och spärras för handläggare innan systemet tas i bruk.

Pseudonymisering nämns särskilt i dataskyddsförordningens artikel 25.1 som en lämplig åtgärd för inbyggt dataskydd. Syftet med pseudonymisering (en process för att dölja identiteter) är att man ska kunna samla ytterligare uppgifter om en och samma individ utan att behöva känna till personens identitet. Pseudonymisering kan ske på ett sätt som går att spåra genom användning av förteckningar över identiteter och deras motsvarande pseudonymer eller genom att använda tvåvägs krypteringsalogoritmer för pseudonymisering. Att dölja identiteter kan också ske på ett sätt så att återidentifiering inte är möjlig, t.ex. genom envägskryptering, som i allmänhet skapar anonymiserade uppgifter. Pseudonymer bör vara slumpmässiga och omöjliga att förutsäga. Spårbara pseudonymiserade uppgifter kan anses som information om individer som är indirekt identifierbara. Kodade uppgifter är ett klassiskt exempel på pseudonymisering. Informationen avser individer som har betecknats med en kod, medan nyckeln för att koppla samman koden och de vanliga identifierarna (namn, födelsedatum och adress) för individerna sparas för sig. Om de koder som används är unika för varje enskild person uppstår en risk för identifiering vid varje tillfälle som det är möjligt att få tillgång till den nyckel som används för krypteringen. Om däremot koderna inte är unika, utan samma koder används för att beteckna individer i olika kommuner och för uppgifter från olika år kan den personuppgiftsansvarige eller en tredje part endast identifiera en viss individ om de vet vilket år och vilken kommun som uppgifterna avser. Om denna tilläggsinformation har försvunnit, och den rimligen inte kommer att återfinnas, kan det anses att informationen inte avser identifierbara individer.

Beträffande användning av personbeteckning finns det bestämmelser i landskapslagstiftning.

4.2. Begränsning av åtkomsten till uppgifterna

Att låta alla register och sökmöjligheter vara helt öppna för samtliga tänkbara användare medför stora integritetsrisker jämfört med att låta åtkomsten styras och begränsas av arbetsflödet. Möjligheten att arbeta med och ta del av personuppgifter bör begränsas till att endast avse anställda som behöver uppgifterna för att kunna utföra sina arbetsuppgifter. IT-system bör vara utformade med behörighetsstyrning som kan anpassas efter organisationens arbetssätt, så att personalen inte får befattning med personuppgifter som inte är arbetsrelaterade. Begränsningen av information kan vara baserad på innehav av roller eller medlemskap i grupper. Utöver behörighetssystem kan även kryptering av lagrad information vara ett sätt att begränsa åtkomsten för t.ex. systemadministrativ personal.

4.3. Skydd för uppgifterna

En av principerna för behandling av personuppgifter är, enligt artikel 5.1. i dataskydds-förordningen, att personuppgifterna med användning av lämpliga tekniska eller organisatoriska åtgärder ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. IT-system som hanterar personuppgifter ska redan från början ha stöd för säkerhetsfunktioner. Särskilt tjänster som exponeras mot internet måste utvecklas med säkerhet som grundfilosofi och så långt det är möjligt vara byggda för att kunna motstå förekommande typer av angrepp. Att lägga till säkerhetsfunktioner, särskilt oplanerade sådana, i efterhand kan bli dyrt och orsaka driftsstörningar.

Ju känsligare uppgifter, desto högre säkerhetsnivå krävs. Utöver behörighetsstyrning bör det exempelvis finnas:

- funktioner för autentisering, minst lösenord, med tillhörande rutiner och funktioner för säker hantering och möjlighet att ansluta systemet till extern kontohantering såsom t.ex. TUPAS eller BankID/ e-legitimation
- möjlighet att använda kryptering vid kommunikation över internet, i databaser, och på mobila enheter
- rutiner och tydlig information om säkerhet till systemets användare
- en logg som kan användas till att utreda felaktig åtkomst till personuppgifter
- stöd för säkerhetskopiering
- säker utplåning, d.v.s. skydd mot att data läcker ut efter att hela eller delar av systemet tagits ur drift och skrotats. Även metoder för radering och förstöring av lagringsmedia bör inkluderas.

Tänk också på att loggar och säkerhetskopior är fristående delar och i sig kan innebära en integritetsrisk. Loggar innehåller personuppgifter om de som arbetar i systemet och måste därför hanteras på ett integritetssäkert sätt.

Säkerhetskopior som sparats länge kan komma att innehålla personuppgifter som borde ha raderats tidigare. Möjligen kan automatiska metoder för gallring komma att behövas.

4.4. Ett system som styr användaren rätt

Ett system som är användarvänligt är i allmänhet integritetssäkrat. Det är viktigt att bygga in användarvänligheten och integritetsskyddet från början. Följande bör tas i beaktande:

- Det bör finnas ”dataskydd som standard” - varvid systemets grundinställningarna är satta så att inte mer information än nödvändigt samlas in eller visas samtidigt som arbetsflöde automatiskt styr användaren mot ett integritetssäkert arbetssätt.
- I användargränssnittet bör det finnas funktioner som begränsar möjligheten att skriva in sådant som inte får skrivas in. T.ex. bör ett skolsystem för elevomdömen utformas så att antalet fritextfält begränsas. Risken för onödiga och olämpliga tillägg minskar på detta sätt.
- Det bör finnas stöd för samtycke och återtagande av samtycke. I många fall krävs samtycke för att registrera viss information eller för att vissa funktioner ska få användas. Se Datainspektionens allmänna råd beträffande hur myndigheterna ska inhämta samtycke från personer vars personuppgifter registreras.
- Utdrag för rapporter eller statistik ska enbart innehålla information som är relevant. Anonymisering kan användas.
- Rättssäkerheten blir högre om de registrerade personerna får insyn:
  - genom ett gränssnitt där de själva kan få fram information,
  - genom funktioner där de på ett enkelt sätt ska kunna få registerutdrag som visar om deras personuppgifter finns i systemet,
  - genom att det i en logg visas till vilka andra organisationer information har lämnats ut till.
- Myndigheter kan behöva användarvänliga funktioner för att effektivt kunna avskilja data för arkivering.
- Uppgifter som inte längre behövs ska tas bort. Arbetet blir enklare om det finns funktioner för att gallra (radera) uppgifter automatiskt.

5. Säkerhetsnivån

I samband med att olika ärenden aktualiseras hos myndigheterna lämnar den enskilda medborgaren olika digitala spår efter sig. Det kan vara tjänsteansökningar som den enskilde skickar, journalanteckningar vid läkarbesök hos hälsocentralen eller loggdata vid användning av skolportalen. Dessa uppgifter samlas i olika register som innehåller personuppgifter. Det rör sig om uppgifter som endast får användas i det syfte för vilket de insamlats och inte heller får sparas längre än nödvändigt.

Den personuppgiftsansvariga myndigheten är skyldig att vidta såväl tekniska som organisatoriska säkerhetsåtgärder för att skydda de personuppgifter som behandlas. En lämplig säkerhetsnivå för personuppgifterna väljs efter en samlad bedömning utifrån följande faktorer:

- Personuppgifternas känslighet
- Risker med behandlingen, t.ex. ju större mängd data desto större risk
- Möjlighet till teknisk utrustning
- Kostnader för att genomföra åtgärderna

Generellt gäller att ju känsligare personuppgifterna är och ju större riskerna är med behandlingen, desto mer omfattande bör säkerhetsåtgärderna vara.

Vid användandet av e-tjänster måste myndigheten kunna vidta följande säkerhetsåtgärder:

- I de fall det är nödvändigt, säkerställa identiteten hos användaren av en e-tjänst
- Skydda sådana personuppgifter som förs över i öppna nät så att obehöriga inte kan ta del av dem
- Skydda personuppgifter som samlats in.

5.1. Behörighetstilldelning

Det måste finnas fungerande rutiner för behörighetstilldelning och tydliga riktlinjer för när det är tillåtet för personalen att ta del av personuppgifter. En grundläggande princip är att anställda inom en myndighet endast bör ha tillgång till information som de behöver i sitt arbete. Den personuppgiftsansvariga myndigheten bör utforma arbetsrutiner och arbetsuppgifter på ett sådant sätt att det blir möjligt för personalen att arbeta och tänka säkerhetsmedvetet.

5.2. Utbildning

Utbildningsinsatser är av stor betydelse för att hanteringen av personuppgifter ska vara säker. Tekniska säkerhetslösningar är inte effektiva om personalen inte vet hur den får hantera lagrade personuppgifter. Den personuppgiftsansvariga myndigheten måste se till att alla som har tillgång till personuppgifter får relevant utbildning. Utbildningen kan omfatta såväl de tekniska lösningarna och de praktiska arbetsrutinerna som den gällande lagstiftningen.

5.3. Behandlingshistorik

När känsliga personuppgifter behandlas ska det finnas en behandlingshistorik (logg) som löpande registrerar användaridentitet, tidpunkt och vilka personuppgifter användaren har haft åtkomst till eller bearbetat. Det ska vara möjligt att följa upp loggarna för att utreda felaktig eller obehörig användning av personuppgifter.

5.4. Autentisering – kontroll av användarens identitet

Det blir både säkrare och enklare att kunna ingå rättsligt bindande avtal om en myndighet kan slå fast identiteten hos användaren av en e-tjänst. Dessutom minskar risken för att obehöriga ska kunna få del av integritetskänslig information, förvanska information eller lämna felaktiga uppgifter.
Det finns flera metoder för autentisering. Några exempel är personliga lösenord, engångslösenord och e-legitimation. Valet av metod beror bl.a. på hur känsliga de behandlade personuppgifterna är och vilka tänkbara risker som finns med behandlingen.
Behandling av känsliga personuppgifter eller stora mängder personuppgifter kräver säkra metoder för autentisering, såsom e-legitimation, engångslösenord eller motsvarande. I dessa fall räcker inte t.ex. användarnamn och lösenord eller pinkod som metod för autentisering.

5.5. Skydd av känsliga personuppgifter som skickas via öppna nät

Om en myndighet hämtar känsliga personuppgifter via ett öppet nätverk, som t.ex. internet, ska själva överföringen av uppgifterna vara skyddad med hjälp av kryptering. Med kryptering kan myndigheten försäkra sig om att ingen obehörig kan komma åt informationen och att den inte förvanskas på vägen. Personer som ska skicka sina personuppgifter till en myndighet måste kunna identifiera myndigheten och känna trygghet inför att skicka sina uppgifter via internet. Det kan t.ex. åstadkommas genom att använda s.k. servercertifikat och att kryptera trafiken med hjälp av SSL/TLS.

Om en myndighet sänder e-post med känsliga personuppgifter via ett öppet nät, ska informationen krypteras så att endast den avsedda mottagaren kan ta del av personuppgifterna.

Personuppgifterna ska förstås inte bara skyddas när de skickas via internet utan även när de lagras hos myndigheten. För att åstadkomma ett bra skydd krävs både tekniska lösningar och administrativa rutiner.

Detta dokument ersätter Datainspektionen informerar Nr 4/2012, Principer för inbyggt dataskydd (Privacy by design).