Datainspektionen informerar

Nr 4/2012

Principer för inbyggt dataskydd

(Privacy by design)

Användningen av IKT i förvaltningen står högt på den politiska agendan. Flera skolportaler är redan lanserade och användningen av tekniken kommer i allt högre utsträckning att underlätta för medborgarna att kontakta skola, hälsovård och annan offentlig verksamhet.

Datainspektionen har tagit fram en **vägledning för hur IT-system bör utformas** för att redan från början uppfylla kraven i personuppgiftslagen.

Utveckling av tekniska system är ofta komplicerade processer där hänsyn ska tas till olika krav. Ett av kraven är att värna den personliga integriteten. Genom att följa personuppgiftslagen från första början undviker myndigheterna att systemen måste göras om.

Datainspektionen, den 29 november 2012

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 Sammanfattning

Genom att beakta integritetsfrågorna under IT- systemets hela livscykel, från början till slut, kan personuppgiftslagen[1] efterlevas. Samtidigt kommer systemet att hålla en hög säkerhetsnivå. På så sätt undviks ökande kostnader och tidsödande arbetsinsatser med att lindra bristande dataskydd i efterhand.

Inbyggt dataskydd tillämpas på många områden. Denna vägledning riktar sig främst till beställare, leverantörer av produkter och tjänster eller andra som på annat sätt är involverade i framtagningen av IT-stöd för behandling av personuppgifter.

2 Allmänt om e-förvaltning

E-förvaltning definieras som ”verksamhetsutveckling i offentlig förvaltning som drar nytta av informations- och kommunikationsteknik kombinerad med organisatoriska förändringar och nya kompetenser”.

Användningen av IKT i förvaltningen står högt på den politiska agendan. Flera skolportaler är redan lanserade och användningen av tekniken kommer i allt större utsträckning att underlätta för medborgarna att kontakta skola, sjuk- och hälsovård samt annan offentlig verksamhet.

Av landskapsregeringens s.k. omställningsbudget (I tilläggsbudget 2012) framgår att landskapsregeringens vision är en gemensam e-förvaltning för hela den åländska förvaltningen. Landskapsregeringen har t.ex. för avsikt att tillhandahålla bl.a. e-tjänster. I samband härmed aviserar landskapsregeringen även större närvaro i de sociala medierna.

Utvecklingen av e-tjänster (elektroniska tjänster) innebär en ökad datoriserad behandling av personuppgifter. Behandlingen ska följa personuppgiftslagens[2] bestämmelser. Det är således viktigt att säkerställa att behandlingen av personuppgifterna skyddas på ett bra sätt.

3 Inbyggt dataskydd (Privacy by design)

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

Begreppet inbyggt dataskydd innebär att dataskyddet påverkar systemets hela livscykel – från förstudie via design och utveckling till användning och avveckling.

[1] Landskapslag (2007:88) om behandling av personuppgifter inom landskaps- och kommunalförvaltningen
[2] Landskapslagen (2007:88) om behandling av personuppgifter inom landskaps- och kommunalförvaltningen

4 Registeransvar

En myndighet är registeransvarig[3] 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 registeransvariga myndigheten se till att upprätthålla ett gott skydd för de personuppgifter som behandlas i verksamheten.

Personuppgiftslagen tillämpas även på webbsidor som har en s.k. elektronisk blankett – en webbtjänst som sparar personuppgifter. Några exempel på nättjänster enligt vilka en registerbeskrivning ska göras kan vara:

1. Insamling av information genom internet (kundförfrågningar, anmälningsblanketter och insamling av besökarrespons m.m.)
2. Diskussionsfora som förutsätter registrering
3. Annan registrering

Vid insamling av personuppgifter ska den registrerade informeras om den framtida behandlingen av uppgifterna han eller hon lämnar. Information ska ges om åtminstone registeransvarig, ändamål med behandlingen, uppgifter om regelbunden utlämning av uppgifter, vilka rättigheter den registrerade har att bl.a. kontrollera uppgifterna.

I de fall myndigheten lejt ut databehandlingen på en extern näringsidkare ska det finnas ett skriftligt avtal som reglerar hur näringsidkaren ska behandla uppgifterna och vilka säkerhetsåtgärder som ska vidtas.

Till ansvaret hör att se till att det IT-stöd som används inte medför integritetsrisker. Därför 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. Samma gäller om det istället för hårdvara eller programvara är fråga om en tjänst som levereras genom outsourcing eller molntjänster så är beställaren ansvarig och måste se till att leverantören uppfyller kraven på säkerhet och integritetsskydd.

[3] Registeransvarig är den myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter

5 Säkerhetsnivån

Den registeransvariga myndigheten är skyldig att vidta såväl tekniska som organisatoriska säkerhetsåtgärder för att skydda de personuppgifter som behandlas. En lämplig säkerhetsnivå för personuppgifterna uppnås genom att göra 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.

6 Skydd av personuppgifter i e-tjänster

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

7 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.

Känsliga personuppgifter är enligt personregisterlagen sådana som avslöjar:

- Ras eller etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i fackförening
- Personuppgifter som rör hälsa eller sexualliv

Behandling av känsliga 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.

Uppgifter som omfattas av sekretess samt uppgifter om lagöverträdelser bör likställas med känsliga personuppgifter när det gäller säkerhet.

Även andra personuppgifter kan sammantaget vara integritetskänsliga och bör därför skyddas av säkrare typer av autentisering. Det gäller t.ex. om en användare efter inloggning till en e-tjänst kommer åt ett stort antal personuppgifter.

7.1 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. Medborgarna måste även kunna identifiera myndigheten och känna trygghet med 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.

7.2 Skydd av personuppgifter som samlats in via en e-tjänst

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

7.3 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. Tekniska säkerhetslösningar är inte effektiva om personalen inte vet hur den får hantera lagrade personuppgifter. Den registeransvariga bör utforma arbetsrutiner och arbetsuppgifter på ett sådant sätt att det blir möjligt för personalen att arbeta och tänka säkerhetsmedvetet.

7.4 Utbildning

Utbildningsinsatser är av stor betydelse för att hanteringen av personuppgifter ska vara säker. Den registeransvariga bör 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.

7.5 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.

8 Checklista för IT-projekt

Dataskyddet förutsätter en strukturerad arbetsmetod som är jämförbar med IT-säkerhet och kvalitetssäkring. Därför behövs en riskanalys[4] där konsekvenserna för de registrerade individernas integritet kartläggs. Hur säkerhetskravet bedöms framgår av följande.

En myndighet är registeransvarig[5] 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 registeransvariga myndigheten se till att upprätthålla ett gott skydd för de personuppgifter som behandlas i verksamheten.

8.1 Begränsa 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 det skede som uppgifterna samlas in. Ändamålet för behandlingen ska vara bestämt i förväg. Ändamålet för behandlingen är avgörande för vilka krav som ska ställas på systemet.

Integritetsriskerna kan begränsas genom att t.ex.

- Begränsa uppgifterna till att endast indirekt peka ut en individ
- Begränsa uppgifterna till att vara mindre känsliga
- Ersätta namn med t.ex. pseudonymer
- Undvika att rutinmässigt ha med personbeteckning som fält i databaser

Om t.ex. ett ärendehanteringssystem kan göra mer med personuppgifter än vad som är tillåtet enligt ändamålet ska de funktionerna begränsas och spärras för handläggare innan systemet tas i bruk.

8.2 Begränsa åtkomsten till uppgifterna

Arbetssättet bör granskas kritiskt för att säkerställa att det inte är arbetssättet i sig som framtvingats av IT-system med otillräcklig behörighetsstyrning eller andra brister i säkerhet och integritet.

Möjligheten att arbeta med och ta del av personuppgifter ska begränsas till att avse endast de som behöver uppgifterna för att kunna utföra sina arbetsuppgifter. Sättet att arbeta på måste således vara utformat enligt samma princip. IT-system bör vara utformade med behörighetsstyrning som kan anpassas efter organisationens arbetssätt för att undvika befattning med personuppgifter som inte är arbetsrelaterade.

[4] Exempel på riskanalys finns på http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/se/pdf

[5] Registeransvarig är den myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter

Begränsningen av information kan vara baserad på innehav av roller eller medlemskap i grupper. Att låta åtkomsten styras och begränsas av arbetsflödet såsom handläggning av ett ärende hos myndigheten kan minska integritetsriskerna jämfört med att låta alla register och sökmöjligheter vara helt öppna för samtliga användare. Utöver behörighetssystem kan även kryptering av lagrad information vara ett sätt att begränsa åtkomsten för t.ex. systemadministrativ personal.

8.3 Skydda uppgifterna

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. http://tupas.fi 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.

8.4 Låt systemet styra användaren rätt

Det är viktigt att bygga in integritetsskyddet från första början. Personlig integritet ska vara en drivande faktor vid t.ex. val av skyddsnivåer och åtgärder. Förtydliga hur balans kan skapas mellan å ena sidan personlig integritet och å andra sidan säkerhetsåtgärder som kan vara kränkande, t.ex. loggning och annan övervakning.

Några exempel på integritetsskyddande åtgärder kan vara:

- ”Integritet som standard” - systemets arbetsflöde styr användaren automatiskt mot ett integritetssäkert arbetssätt och att grundinställningarna är satta så att inte mer information än nödvändigt samlas in eller visas.

- Uppgifter som inte längre behövs ska tas bort. Funktioner för att gallra (radera) uppgifter automatiskt förenklar.

- Myndigheter kan behöva användarvänliga funktioner för att effektivt kunna avskilja data för arkivering.

Transparens – genom att ge de registrerade insyn:

  - genom funktioner så att de registrerade på ett enkelt sätt ska kunna få lagstadgade registerutdrag som visar om deras personuppgifter finns i systemet
  - genom ett gränssnitt för att låta den registrerade själv få insyn
  - genom att i en logg enkelt kunna visa till vilka andra organisationer information har lämnats ut.

- Utdrag för rapporter eller statistik ska inte innehålla information som inte är relevant. Anonymisering kan användas.

- 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.

- Funktioner i användargränssnittet 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 otillåtna och kränkande omdömen minskar på detta sätt.

- Tydlig information om hur uppgifterna kommer att behandlas. Informationen ges till de som lämnar uppgifter om sig själva.

9 Vårt mål

Datainspektionen är en myndighet som arbetar för att medborgarnas personliga integritet inte kränks när personuppgifter behandlas. Myndigheten finns till för medborgarna.

Vi arbetar också proaktivt genom att informera myndigheterna om deras skyldighet att hantera personuppgifter på ett korrekt sätt. Bland annat ska myndigheterna informera om hur de behandlar personuppgifter. I vårt arbete ingår också att ge allmänna råd.

Vi utbildar och informerar myndigheterna om användningen av personuppgifter. Myndigheterna har en skyldighet att göra upp beskrivningar över vilka personregister de för inom myndigheten. Registerbeskrivningarna ska hållas tillgängliga för var och en.