



# IT-säkerhet och myndigheters e-tjänster

Allt fler myndigheter utvecklar nu elektroniska tjänster eller e-tjänster som det brukar kallas. Några exempel på e-tjänster är möjligheten att låna böcker, begära föräldrapenning, lämna synpunkter och klagomål till en kommuns anställda eller förtroendevalda eller att följa sitt ärende via webben. Även tjänster av typen "Mina sidor" och elevadministrativa system räknas som e-tjänster.

Utvecklingen av e-tjänster innebär en ökad datoriserad behandling av personuppgifter. Den här behandlingen måste följa reglerna i personuppgiftslagen (PuL), särskild registerlagstiftning och sekretesslagstiftningen. För myndigheter som inför e-tjänster är det viktigt att säkerställa att personuppgifterna skyddas på ett bra sätt. Syftet med det här dokumentet är att informera om de krav som personuppgiftslagen ställer i fråga om säkerhet samt att ge råd och vägledning till myndigheter i deras arbete med säkerheten kring e-tjänster.

## 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 myndigheten behandlar uppgifter som lämnas till myndigheten eller när sådana e-tjänster som "Mina sidor" erbjuder möjligheter för den enskilde att på myndighetens webbplats registrera uppgifter. Den personuppgiftsansvarige ska se till att upprätthålla ett gott skydd för de personuppgifter som behandlas i verksamheten.

Om myndigheten får hjälp med databearbetningen av exempelvis en extern servicebyrå så kan det företaget bli så kallat personuppgiftsbiträde. I sådana fall ska det finnas ett skriftligt avtal som reglerar hur biträdet ska behandla uppgifterna och vilka säkerhetsåtgärder som ska vidtas.



## Samlad bedömning avgör säkerhetsnivån

Den personuppgiftsansvarige är skyldig att vidta säkerhetsåtgärder, såväl tekniska som organisatoriska, för att skydda de personuppgifter som behandlas. För att skapa ett lämpligt skydd för personuppgifterna gäller det att göra en samlad bedömning som tar hänsyn till:

- Hur pass känsliga de behandlade personuppgifterna är (se mer längre fram)
- De risker som finns med behandlingen av personuppgifterna. En behandling av uppgifter om många personer kan exempelvis leda till mer omfattande skador vid ett angrepp på säkerheten
- De tekniska möjligheter som finns tillgängliga på marknaden
- Vad det kostar att genomföra åtgärderna

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

## Skydd av personuppgifter i e-tjänster

När det gäller e-tjänster är det framför allt tre säkerhetsaspekter som är viktiga. Myndigheten måste 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
- skydda personuppgifter som samlats in

### **Fastställa identiteten hos användaren – autentisering**

Om en myndighet kan slå fast identiteten hos användaren av en e-tjänst blir det både säkrare och enklare att kunna träffa rättsligt bindande avtal. Dessutom minskar risken för att obehöriga ska kunna få del av integritetskänslig information, förvanska information eller lämna felaktiga uppgifter.

Det finns en rad metoder för autentisering, som exempelvis personliga lösenord, engångslösenord och e-legitimation. Vilken metod för autentisering som krävs för en e-tjänst beror bland annat på hur känsliga personuppgifterna är som hanteras och vilka tänkbara risker som finns med behandlingen.

Känsliga personuppgifter är enligt personuppgiftslagens definition 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 det inte med exempelvis 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 personuppgifter vilka enligt personuppgiftslagen inte definieras som känsliga kan sammantaget vara integritetskänsliga och bör därmed skyddas av säkrare typer av autentisering. Det gäller exempelvis om en användare efter inloggning till en e-tjänst kommer åt ett stort antal personuppgifter.

I Datainspektionens informationsblad "Personuppgifter och e-förvaltning, Vägledning för kommuner" listas ett antal exempel på e-tjänster som normalt sett innebär större risker i integritetshänseende och som följaktligen kräver mer avancerade metoder för autentisering.



### **Skydd av känsliga personuppgifter som skickas via öppna nät**

Ska en myndighet hämta in känsliga personuppgifter via ett öppet nätverk, som till exempel Internet, måste själva överföringen av uppgifterna vara skyddad med hjälp av kryptering. Med kryptering kan myndigheten säkerställa 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. Detta kan åstadkommas genom att använda så kallade 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.

### **Skydd av personuppgifter som samlats in via en e-tjänst**

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

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

**Utbildning** – Utbildningsinsatser är av stor betydelse för att hanteringen av personuppgifterna ska vara säker. Den personuppgiftsansvarige 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.

**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.

## Mer information om e-tjänster och säkerhet

På Datainspektionens webbplats kan du läsa mer om om e-tjänster och säkerhet. Adressen är [www.datainspektionen.se/e-forvaltning](http://www.datainspektionen.se/e-forvaltning). Där kan du också ladda ner följande informationsmaterial:

- Personuppgifter och e-förvaltning, Vägledning för kommuner. April 2007.
- E-förvaltning och personuppgiftslagen. Informationsblad. Februari 2008.
- Informationssäkerhet, Informationsblad. September 2006.
- Säkerhet för personuppgifter, Allmänna råd. December 1999.

Dessa kan även beställas i tryckt form på webbplatsen eller på telefon 08-657 61 15.

## Kontakta Datainspektionen

E-post: [datainspektionen@datainspektionen.se](mailto:datainspektionen@datainspektionen.se) Webb: [www.datainspektionen.se](http://www.datainspektionen.se)  
Tfn 08-657 61 00. Postadress: Datainspektionen, Box 8114, 104 20 Stockholm.

