Datainspektionen informerar

Nr 1/2013

E-postanvändning

Användningen av elektronisk post (e-post) tar alltmer över som kommunikationsmedel. Ofta uppkommer frågeställningar kring hur myndigheterna bör behandla information som sänds med e-post och som innehåller personuppgifter. Många gånger är det fråga om känsliga personuppgifter som skickas till myndigheterna.

Det ska vara enkelt att göra rätt. Därför har Datainspektionen tagit fram en **vägledning för hur myndigheter bör förhålla sig till användningen av e-post**.

Datainspektionen

den 20 maj 2013

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

Tekniken underlättar och hjälper oss som individer. Tekniken kan dock missbrukas på ett sätt som är negativt för vår personliga frihet. Det kan röra sig om identitetsstöld, kartläggning av en individs privatliv, avlyssning med mera. System och teknik bygger på att vi själva sätter gränserna för vad som är acceptabelt. Ju tydligare vi är, desto bättre skydd får vi.

Det finns många områden där känsliga personuppgifter behandlas. Det gäller bland annat inom hälso- och sjukvård, socialförvaltning och utbildning. De här uppgifterna lagras och behandlas på olika sätt med hjälp av teknik. Det är viktigt att det görs på ett säkert sätt. Ett sjukhus måste givetvis veta så mycket som möjligt om en patients hälsotillstånd, men vilka konsekvenser får det för den enskilde om försäkringsbolaget eller arbetsgivaren får reda på samma sak?

Vid hantering av e-post finns det alltid en risk för att andra än den avsedda mottagaren kan ta del av meddelandet. Därför är det viktigt att ha rutiner för hur e-posten behandlas.

En dokumenterad policy, utöver tydliga instruktioner till användarna, minskar riskerna för kränkningar och underlättar hanteringen av e-post. Instruktionerna ska vara så tydliga att det klart framgår vilka typer av personuppgifter som under vilka omständigheter får respektive inte får skickas med e-post. Eventuella referenser till sekretessmarkerade, skyddsvärda eller känsliga uppgifter bör förtydligas så att tvivel kring vad som avses undviks. Eftersom inkommande e-post kan innehålla integritetskänsliga personuppgifter behövs rutiner för att ta hand om den. E-postsystem är normalt inte konstruerade för att hantera den typen av personuppgifter.

För att en policy ska förbli verkningsfull bör det även finnas rutiner för att säkerställa att den efterlevs.

Myndigheternas datateknik bör utvecklas så att elektroniska system utarbetas för uträttande av ärenden så att klienternas meddelandehemlighet bibehålls.

2 E-post

Utgångspunkten är att e-post är okrypterad, vilket betyder att det kan vara möjligt för andra att läsa innehållet. Enkelt kan okrypterad post jämföras med att sända ett vykort. Sådan information som du inte skulle skriva på vykort, bör du inte heller skicka i e-post. Exempel på sådan information som du inte ska skicka är uppgifter om hälsa.

För att garantera säkerheten för överföring och lagring av känsliga personuppgifter behöver myndigheterna implementera fasta säkerhetsrutiner såsom till exempel användning av säkra metoder för konfigurering, kopplingsverktyg samt inloggnings- och överföringsprotokoll.

2.1 Särskilda risker med e-post

Det finns särskilda risker med hantering av personuppgifter i e-post eftersom det är svårt att försäkra sig om att endast den avsedda mottagaren kan ta del av meddelandet. I många fall är det omöjligt att säkerställa identiteten hos en mottagare enbart utifrån en e-postadress. Det finns dessutom stor risk för säkerhetsbrister i de kommunikations-protokoll som ligger till grund för e-postsystem. När ett e-postmeddelande skickas mellan e-postservrar över internet passerar det ofta andra servrar[1] på vägen. Om informationen i e-postmeddelandet är oskyddad finns det inget som hindrar att kopior av informationen sparas undan vid var och en av dessa servrar. Kopior av mottagna och skickade e-postmeddelanden ligger ofta kvar i enskilda användares brevlådor, både i e-postprogram i såväl fasta och mobila enheter och i servrar. Det blir då ännu svårare att undvika att obehöriga tar del av dem. Det gäller särskilt om e-posten är åtkomlig via ett öppet nät eller är synkroniserad med mobila enheter, till exempel bärbara datorer, pekplattor och mobiltelefoner.

Dagens e-postprogram innehåller också en del funktioner som ökar riskerna för att e-postmeddelanden skickas fel. Det kan vara namn och e-postadresser som fylls i automatiskt eller upprättade e-postlistor som gör att e-posten oavsiktligt riskerar att skickas till fel mottagare eller till betydligt fler mottagare än avsändaren avsett.

2.2 Intern hantering av e-post

Frågan om det är någon skillnad mellan att skicka känsliga personuppgifter i e-post till någon inom den egna organisationen eller till någon utanför. Bakom frågan ligger ofta en uppfattning om att e-post som skickas inom en organisation inte går över öppna nät och att någon särskild hänsyn därför inte skulle behövas. Utöver de särskilda risker som beskrivs ovan och behovet av att ha tydliga instruktioner genom att ha tydliga säkerhetsrutiner så har teknikutvecklingen inneburit att resonemang kring intern e-post hos många organisationer alltmer förlorat sin relevans.

Om det finns funktioner för webbmail innebär de så gott som alltid att e-post görs tillgängligt via ett öppet nät. Det gäller också när e-post, utan att gå över ett virtuellt privat nätverk, kan hämtas till e-postklienter utifrån via till exempel POP eller IMAP. Detsamma gäller om vissa tjänster, till exempel antivirusfunktioner eller spamtvätt, tillhandahålls av en extern leverantör. Om hela eller delar av drift, administration eller underhåll av e-postsystemet läggs ut på en extern part uppstår frågor om hur denna går till väga för att logga in till e-postsystemet. Funktioner för distansadministration används ofta över öppet nät.

Den ökade användningen av och synkroniseringen med mobila enheter gör också att det blir allt svårare att tala om intern hantering av e-post eftersom sådana ofta används utanför den egna organisationens utrymmen och nätverk.

[1] Personuppgifter, t.ex. e-post, fotografier och elektroniska kalendrar kan skapas t.ex. på Åland med hjälp av ett mjukvaruprogram vars värdserver finns i Tyskland, bearbetas i Indien, lagras i Polen och tas fram i Spanien av en italiensk medborgare

3 Förvaltningslagen

Enligt förvaltningslagen ska myndigheter se till att det är möjligt för enskilda att kontakta dem med hjälp av e-post och att svar får lämnas på samma sätt. Det är myndigheten som i det enskilda fallet avgör på vilket sätt ett svar på ett e-postmeddelande ska lämnas. Myndigheten har ingen skyldighet att lämna svaret per e-post och det finns situationer då det är lämpligare att svaret lämnas på annat sätt. Exempel på sådana situationer är om svaret innehåller hemliga uppgifter eller som på annat sätt är integritetskänsliga och myndigheten inte kan skydda dem på ett sådant sätt att endast den avsedda mottagaren kan ta del av dem.

4 Användning av e-post inom socialvården

Socialvårdshandlingar som innehåller uppgifter om socialvårdsklienter eller andra enskilda ska hållas hemliga. En sekretessbelagd handling eller en kopia eller utskrift av en sådan handling får inte visas för eller lämnas ut till utomstående eller på något annat sätt visas för eller lämnas ut till utomstående (14 § 1 o 2 mom. lagen om klientens ställning och rätigheter inom socialvården FFS 812/2000).

Den som ordnar eller producerar socialvård[2] samt den som är anställd hos denne, liksom den som har ett förtroendeuppdrag inom socialvården, får inte röja en uppgift som vore sekretessbelagd om den ingick i en handling, och inte heller någon annan omständighet som han eller hon har fått kännedom om i samband med uppdrag inom socialvården och för vilken tystnadsplikt föreskrivs genom lag. En uppgift för vilken tystnadsplikt gäller får inte heller röjas efter det att verksamheten hos dem som ordnar eller producerar socialvård har upphört eller det uppdrag som utförts för dennes räkning har avslutats (15 §).

Uppgifter ur en sekretessbelagd handling får lämnas ut med klientens uttryckliga samtycke eller såsom särskilt bestäms i lag. När klienten saknar förutsättningar att bedöma betydelsen av samtycket, får uppgifter lämnas ut med samtycke av klientens lagliga företrädare. Uppgifter får emellertid inte lämnas ut med samtycke av en minderårig klients lagliga företrädare, om företrädaren själv inte har rätt att få informationen av en anledning som avses i 11 § 3 mom.

Den registeransvariga ska skydda personuppgifterna från utomstående bl.a. med tillräckliga tekniska åtgärder. Det gäller även då de skickas med e-post. Detta gäller trots att den registrerade givit sitt samtycke. Uppgiften om ett klientförhållande är sekretessbelagd. Socialmyndigheten kan skicka meddelanden per e-post endast om klienten använder e-post som är tillräckligt krypterad och parterna kan identifieras[3].

[2] Vad avser hälso- och sjukvårdsproducenter i offentlig regi har Datainspektionen publicerat vägledning i Allmänna råd nris 4/2011 och 3/2012 http://www.di.ax/vara-rad?start=1

[3] Riksdagens justitieombudsmans beslut 12.11.2009 704/4/08)

5 Informationssäkerhet och rutiner

Känsliga personuppgifter får endast lämnas ut via öppna nät till identifierade användare vars identitet är säkerställd med en teknisk funktion som asymmetrisk kryptering (till exempel e-legitimation), engångslösenord eller motsvarande. Dessutom ska känsliga personuppgifter vara krypterade vid överföring.

Många webbsidor på myndighetsservern har en ”kontakt”-knapp som aktiverar medborgarens e-postprogram för kommentarer till en särskild e-brevlåda. Det finns en vision om en väl utvecklad webbplats, där allmänheten efter inloggning kan ta del av ett varierat utbud av e-tjänster såsom möjligheten att följa sitt eget ärende via myndighetens webbplats eller ansöka om barnomsorg. Detta förfaringssätt kräver metoder för säker identifiering av användaren. Många myndigheter använder fortfarande sina webbplatser huvudsakligen som informationskanal och inte som verktyg för tvåvägskommunikation mellan medborgare och förvaltning. Det finns också myndigheter som erbjuder möjligheten att fylla i enklare formulär och att ladda hem blanketter för underskrift.

När ett e-postmeddelande skickas registreras avsändarens personuppgifter endast i den omfattning som behövs för att svara på frågan och därefter vidarebefordras meddelandet. Avsändaren underrättas sedan via e-post om vart meddelandet skickats. Om det finns frågor om hur e-postmeddelandet och avsändarens personuppgifter behandlas kan frågorna skickas tillsammans med meddelandet.

Om myndighetens eller enskild tjänstemans e-postadress är tillgänglig på internet bör information finnas om för vilket ändamål e-posten kan användas och om de dataskyddsproblem som är kopplade till användningen av e-post som är öppen och internetbaserad utan kryptering av meddelande och där avsändaren kan identifieras. Behovet av åtgärder och policy för att minska säkerhetsrisker vid användning av elektronisk post bör övervägas.

Reparation och service bör utföras på ett sådant sätt att personuppgifter inte blir tillgängliga för obehöriga. Avtal med serviceföretaget om utomstående ska reparera eller göra underhållservice av IT-utrustning är nödvändigt. Avtalet bör anpassas till hur känsliga personuppgifter som finns i systemet. Avtalet kan också innehålla bestämmelser om vilka säkerhetsrutiner som ska tillämpas i samband med servicen. Samma sak gäller när datamedia tas ur bruk.

Förslag på hur en informationssäkerhetspolicy kan se ut har svenska post- och telestyrelsen tagit fram på http://www.pts.se/sv/Internet/Internetsakerhet/For-arbetsplatsen/Uppratta-policy/
Av dokumentet framkommer bland annat att åtminstone följande uppgifter bör finnas med, nämligen:

5.1 Elektronisk post

E-posten som arbetsverktyg är en kommunikationsmetod som ofta använder internet. Användningen av internet innebär vissa risker: E-brev kan ”avlyssnas” och innehåll eller avsändare kan ändras av obehöriga. Dessutom är e-post ett mycket vanligt sätt att sprida skadlig kod. Tänk på vilka som ska ha tillgång till e-post, vilken information som får skickas med e-post, skydd mot skadlig kod, hantering av bifogade filer, kryptering med mera.

5.2 Behörighetsadministration/styrning av åtkomst

Riktlinjer för vem som ska komma åt vad och hur arbetet med åtkomsten ska skötas i organisationen.

För att skydda informationen bör åtkomsten begränsas. Hoten finns både inom organisationen och utanför den, till exempel leverantörer och konsulter. Ett misstag kan få stora konsekvenser . Det är därför viktigt att åtkomst endast ges till de IT-system som respektive användarkategori behöver och kan använda. Tänk särskilt på följande: Vem ska ha behörighet till IT-systemen, vad får de komma åt, ändra eller radera i IT-systemen och sin egen dator, vem är ansvarig för att besluta om respektive behörigheter, rutiner för tilldelning, uppföljning och uppdatering av behörigheter.

5.3 Information på webbplats om regler om skydd för personuppgifter

Det finns också skäl att överväga vilka åtgärder och eventuell policy som behövs för säker användning av internet och e-post. Till exempel kan information på myndighetens webbplats formuleras på följande sätt:

> ALTERNATIV 1
> Skriftlig kommunikation med Datainspektionen (e-post, vanlig post eller fax) blir allmän handling och kan komma att diarieföras. E-post till inspektion@di.ax kommer till vår registratur. Myndighetens personal har e-postadresser enligt följande: förnamn.efternamn@di.ax
>
> ALTERNATIV 2
> Datainspektionen har åtagit sig att skydda användarnas personliga integritet. Skyddet för enskilda då Datainspektionen behandlar personuppgifter baseras på landskapslag (2007: 88) om behandling av personuppgifter om landskaps- och kommunalförvaltningen (personuppgiftslagen).
>
> Dessa regler gäller samtliga webbplatser inom domänen di.ax. Även om du kan navigera på de flesta av webbplatserna utan att lämna uppgifter om dig själv, krävs det i bland att du lämnar personuppgifter för att få tillgång till vissa e-tjänster. På webbplatser där personuppgifter krävs, behandlas dessa i enlighet med personuppgiftslagen och information om hur uppgifterna på en webbplats används finns i webbplatsens policy för integritetsskydd.

Varje e-tjänst har en registeransvarig som beslutar om syftet med personuppgiftsbehandlingen. Den registeransvariga ansvarar för att e-tjänsten överensstämmer med webbplatsens policy för integritetsskydd.

Datainspektionen är oberoende tillsynsmyndighet.

6 Checklista

Den registeransvariga myndigheten bör tänka på att:

- Kartlägga hotbilden
- Sätta hållbara mål för säkerhet
- Fastställa policy för säkerhet
- Skapa en fungerande organisation för säkerhet
- Skaffa den utrustning som behövs och använda den rätt
- Upprätta regler och rutiner
- Informera och utbilda kontinuerligt
- Följa upp att regler och rutiner efterlevs och respekteras
- Testa säkerheten regelbundet