Datainspektionen

Datum	Diarienr
2013-05-08	1552-2012

Socialnämnden i
Norrköpings kommun
Rådhuset
601 81 Norrköping

Tillsyn enligt personuppgiftslagen (1998:204) – Behandling av känsliga personuppgifter i mobila enheter

Datainspektionens beslut

Datainspektionen förelägger Socialnämnden i Norrköpings kommun att

- säkerställa att den autentiseringsmetod som används uppfyller kraven på stark autentisering.

Datainspektionen förutsätter att Socialnämnden i Norrköpings kommun

- inför funktioner för att förhindra åtkomst till personuppgifter som inte längre behöver vara tillgängliga via mobila enheter, och
- kompletterar sina instruktioner till användarna i enlighet med vad som framgår av Datainspektionens checklista.

Datainspektionen vill också påminna nämnden om vikten av att löpande göra riskidentifieringar och säkerhetsutvärderingar i sin riskanalys.

Ärendet avslutas.

Redogörelse för tillsynsärendet

Datainspektionen har granskat ett antal socialnämnders behandling av känsliga personuppgifter vid användning av mobila enheter. Syftet har varit att undersöka om nämnderna vidtagit tillräckliga säkerhetsåtgärder för att skydda personuppgifterna som behandlas. Socialnämnden i Norrköpings kommun har beskrivit sin behandling av personuppgifter i mobila enheter

Postadress: Box 8114, 104 20 Stockholm
Besöksadress: Drottninggatan 29, plan 5
Webbplats: www.datainspektionen.se
E-post: datainspektionen@datainspektionen.se
Telefon: 08-657 61 00
Telefax: 08-652 86 52

genom att besvara en skriftlig enkät. Nämnden har till sitt yttrande bifogat två skriftliga manualer. En för nämndsekreteraren och en för slutanvändarna.

Gällande regelverk

Säkerhet för personuppgifter som behandlas i socialtjänstens verksamhet regleras i 31 § personuppgiftslagen (PuL). Enligt denna bestämmelse är den personuppgiftsansvarige skyldig att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda uppgifterna som behandlas. Den ansvarige ska vara medveten om vilka risker en behandling medför och se till att vidta lämpliga säkerhetsåtgärder för att skydda uppgifterna. Känsligheten hos de personuppgifter som behandlas är en viktig faktor för skyddsnivån. Grundläggande vid överföring av känsliga personuppgifter via öppet nät är att uppgifterna ska skyddas genom exempelvis kryptering och att mottagarens, dvs. den som tar del av uppgifterna, identitet kan säkerställas. Mottagarens identitet ska säkerställas genom någon form av stark autentisering exempelvis engångslösenord, e-legitimation eller motsvarande.

Känsliga personuppgifter är uppgifter som avslöjar

- ras eller etniskt ursprung,
- politiska åsikter,
- religiös eller filosofisk övertygelse,
- medlemskap i fackförening, samt
- uppgifter som rör hälsa eller sexualliv (13 § PuL).

Uppgifter som inte klassificeras som känsliga enligt 13 § PuL kan ändå vara så pass integritetskänsliga att de, när det gäller kraven på säkerhetsåtgärder, ska jämställas med känsliga personuppgifter. Sådana uppgifter kan exempelvis vara uppgifter om lagöverträdelser, uppgifter om ömtåliga förhållanden eller annan information som rör den enskildes privata sfär.

Kravet på att teckna personuppgiftsbiträdesavtal finns i 30 § och bestämmelser om bevarande av personuppgifter regleras i 9 § i) PuL.

Allmänt om behandling av känsliga personuppgifter i mobila enheter

En organisation som vill hantera känsliga eller integritetskänsliga personuppgifter (härefter används enbart benämningen integritetskänsliga personuppgifter) i mobila enheter måste vara medveten om att detta kan innebära vissa särskilda risker. Risker som kan få svåra konsekvenser för en enskild vars personuppgifter riskerar att spridas. En mobil enhet, t.ex. en surfplatta eller en smart telefon, kommunicerar över öppna nätverk och används ofta utanför arbetsgivarens (den personuppgiftsansvarige) lokaler. Det går att utnyttja ett stort antal olika tjänster och ladda ner appar. Appar

kan dock påverka säkerheten i den mobila enheten och medföra oavsiktlig spridning av personuppgifter.

Mobila enheter är som regel stöldbegärlig egendom. Om personuppgifterna i enheten inte är tillräckligt skyddade kan det vara svårt att avgöra om det är den behörige användaren eller någon annan som tar del av uppgifterna. Den ansvarige måste, så långt det är möjligt, vidta säkerhetsåtgärder för att bara en behörig användare ska få åtkomst till personuppgifterna ifråga.

För att den personuppgiftsansvarige ska ha möjlighet att vidta nödvändiga säkerhetsåtgärder vid användning av nya program och tjänster är det viktigt att ha kontinuerlig bevakning och utvärdering av utvecklingen på marknaden. Datainspektionen har tagit fram en checklista för att underlätta för den som planerar att använda sig av mobila enheter för överföring av integritetskänsliga personuppgifter. Den personuppgiftsansvariges skyldigheter är samma även för anställda som tillåts använda sina egna mobila enheter.

- **Riskanalys**
  När personuppgifter behandlas finns det alltid en risk att uppgifterna förstörs, ändras, går förlorade eller att någon obehörig får tillgång till dem. Detta kan bero på olyckshändelse eller att uppgifterna har hanterats på ett otillåtet sätt. För att så långt som möjligt skydda de uppgifter som behandlas måste den personuppgiftsansvarige, innan behandlingen påbörjas, genomföra en riskanalys. I riskanalysen ska man identifiera vilka allmänna och särskilda risker som finns med behandlingen av integritetskänsliga personuppgifter i mobila enheter. Därefter gör man en analys av vilka tekniska och organisatoriska säkerhetsåtgärder som måste vidtas för att hantera dessa risker. Målet är att den personuppgiftsansvarige ska vara medveten om riskerna och ha kontroll över personuppgiftsbehandlingen.
- **Utbildning och instruktioner till användarna**
  Ta fram skriftliga instruktioner om hur det är tillåtet att använda mobila enheter. Instruktionerna bör exempelvis omfatta information om
  - hur integritetskänsliga personuppgifter får hanteras,
  - vilka säkerhetsinställningar som ska användas,
  - eventuella begränsningar för privat användning,
  - vilka appar som är tillåtna att ladda ned, samt
  - vilka konsekvenser otillåten användning kan medföra.

  Den ansvarige behöver också säkerställa att anställda och uppdragstagare som använder sig av mobila enheter får löpande information och utbildning i hur det är tillåtet att hantera enheterna.

- **Behörighetsstyrning**
  För att minimera risken för spridning av integritetskänsliga personuppgifter är det viktigt att begränsa åtkomsten till uppgifterna i fråga. Enbart den som har behov av uppgifterna för att fullgöra sitt uppdrag eller sina arbetsuppgifter ska få åtkomst till uppgifterna.
- **Autentisering och kryptering**
  Om integritetskänsliga personuppgifter är eller kan göras åtkomliga över öppet nät krävs att inloggning sker med stark autentisering såsom e-legitimation, engångslösenord eller liknande. Även inloggning till administrationsgränssnitt kräver stark autentisering. När man använder öppna nät för att hantera integritetskänsliga personuppgifter, ska uppgifterna skyddas genom exempelvis kryptering.
- **Lagring på en mobil enhet**
  Integritetskänsliga personuppgifter som lagras i en mobil enhet ska vara krypterade. Den ansvarige behöver även kontrollera att informationen som lagras i den mobila enheten inte oavsiktligt kopieras och lagras i molnet. När det inte längre är nödvändigt att lagra uppgifterna i de mobila enheterna ska de raderas. I den mån detta inte görs automatiskt ska det finnas skriftliga rutiner som stöd för den manuella hanteringen.
- **Specifika säkerhetsåtgärder för mobila enheter**
  Användning av mobila enheter är förenad med särskilda säkerhetsrisker. För att hantera dessa behöver specifika säkerhetsåtgärder övervägas. Sådana åtgärder kan exempelvis vara att införa
    - Lösenordslås,
    - automatisk låsning av enheten efter viss tids inaktivitet,
    - centrala spärrfunktioner eller distansradering vid händelse av att den mobila enheten tappas bort eller blir stulen,
    - central styrning av säkerhetsinställningar och begränsning för vilka appar som kan laddas ned.
- **Loggning och logguppföljning**
  Som vid all behandling av personuppgifter måste den personuppgiftsansvarige kunna kontrollera vem eller vilka som har haft åtkomst till personuppgifter via en mobil enhet. IT-systemen ska därför kunna generera loggar som regelbundet ska kontrolleras. För att få en förebyggande effekt ska användarna informeras om att loggar kontrolleras regelbundet.
- **Begränsa åtkomsten till personuppgifter**
  När det inte längre finns behov av att hålla personuppgifter tillgängliga via en mobil enhet ska den ansvarige se till att användarna inte längre får åtkomst till uppgifterna i fråga.

- **Personuppgiftsbiträdesavtal**
  Den som använder sig av en tredje part, ett s.k. personuppgiftsbiträde, för behandling av personuppgifter ska teckna ett personuppgifts-biträdesavtal med denna part. Avtalet ska bland annat innehålla instruktioner för biträdets personuppgiftsbehandling och vilka säkerhetsåtgärder biträdet ska vidta.

Datainspektionens bedömning och skäl för beslutet

1. *Allmänt*

Nämnden erbjuder mobila enheter (iPads) till samtliga nämndledamöter för att de ska kunna ta del av elektroniska handlingar inför och under sammanträden. För distribuering av sammanträdeshandlingar används appen ”Mina möten”. Appen ger användaren behörighet att läsa de sammanträdeshandlingar som är knutna till respektive användares möten.

De elektroniska handlingarna laddas upp av nämndsekreteraren som har särskild behörighet för detta. Offentliga handlingar som inte omfattas av sekretess lagras i den mobila enhetens filsystem. Sekretesskyddade handlingar lagras aldrig i plattan.

2. *Riskanalys*

Datainspektionen ser positivt på att nämnden har genomfört en risk- och sårbarhetsanalys. Datainspektionen rekommenderar att nämnden fortlöpande arbetar med riskidentifiering och säkerhetsutvärdering. Detta för att möta nya risker i personuppgiftsbehandlingen i samband med exempelvis organisatoriska förändringar eller ändringar i hanteringen av personuppgifter.

Nämnden har anfört att IT-enheten har genomfört en risk- och sårbarhetsanalys.

3. *Instruktioner till användarna*

Datainspektionen ser positivt på att nämnden tagit fram en skriftlig manual till användarna och att användarna i ett skriftligt avtal förbinder sig att följa kommunens riktlinjer. Datainspektionen förutsätter att nämnden kompletterar sin manual i enlighet med vad som framgår av Datainspektionens checklista.

Nämnden har tagit fram en manual med praktiska instruktioner till användarna om hur appen ”Mina möten” installeras och används. Samtliga

användare måste också genomgå en utbildning om hur den mobila enheten ska hanteras. I ett nyttjandeavtal, som användaren tar del av och undertecknar, anger kommunen sina riktlinjer för användning och hantering av kommunens IT-utrustning. Nämnden har också tagit fram en skriftlig manual för nämndsekreteraren som ansvarar för att lägga in handlingarna i ”Mina möten”.

Den personuppgiftsansvarige ska vidta lämpliga organisatoriska säkerhetsåtgärder (31 § PuL). Att utfärda instruktioner till användarna om exempelvis tillåten behandling av personuppgifter är en sådan säkerhetsåtgärd (se även 30 § PuL).

4. Autentisering och kryptering

Datainspektionen förelägger nämnden att säkerställa att den autentiseringsmetod som används uppfyller kraven på stark autentisering.

Möteshandlingar överförs till mobila enheter via https och certifikat som finns på server och mobil enhet. För att användaren ska beviljas åtkomst till dokumenten i ”Mina möten” måste den mobila enheten först låsas upp med en PIN-kod. Inloggning till ”Mina möten” sker med hjälp av användarnamn och lösenord. Vid första inloggningen i ”Mina möten” knyts varje användare med ett unikt ID till den mobila enhet som han eller hon använder. För att beviljas åtkomst till sekretessbelagda handlingar i ”Mina möten” krävs ytterligare en inloggning. Samma användarnamn och lösenord används. Handlingar med integritetskänsliga personuppgifter strömmas till den mobila enheten. Om användaren varit inaktiv i 10 minuter sker en automatisk utloggning.

När känsliga personuppgifter görs tillgängliga för användare över öppna nät ska användarnas identitet säkerställas med en teknisk funktion som ger en stark autentisering (31 § PuL). Det kan uppnås med hjälp av användarcertifikat (till exempel e-legitimation eller SITHS-certifikat), engångslösenord eller motsvarande. Tillräckligt stark autentisering skulle också kunna uppnås om det är möjligt koppla en mobil enhet till ett tillhörande lösenord eller PIN-kod och på så sätt få en s.k. tvåfaktorsautentisering.

5. *Förhindra åtkomst till personuppgifter som inte längre är nödvändiga*

Datainspektionen konstaterar att nämnden saknar rutiner för förhindra åtkomst till personuppgifter som inte längre är nödvändiga att hålla tillgängliga via surfplattan. Datainspektionen förutsätter att nämnden inför rutiner för att förhindra åtkomst till sådana personuppgifter.

En grundläggande princip i personuppgiftslagen (9 § i)) är att personuppgifter inte ska bevaras längre än nödvändigt. När integritetskänsliga personuppgifter är åtkomliga via mobila enheter är det extra viktigt att det finns rutiner och funktioner för att förhindra åtkomst till sådana uppgifter som inte längre behöver vara tillgängliga via mobila enheterna. För att minimera risken för spridning av uppgifterna bör man begränsa den information som hålls tillgänglig via mobila enheter så mycket som det är faktiskt och praktiskt möjligt.

Av nämndens enkätsvar framgår att sekretessbelagda handlingar inte lagras i appen ”Mina möten”. Det framgår dock inte om nämnden har tagit fram funktioner för att förhindra åtkomst till handlingar som innehåller integritetskänsliga personuppgifter när det inte längre finns något behov av åtkomst till uppgifterna. Även när det gäller personuppgifter som förekommer i offentliga handlingar måste nämnden ta ställning till hur länge dessa ska vara åtkomliga i de mobila enheterna.

Hur man överklagar
Om ni vill överklaga beslutet skall ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Överklagandet skall ha kommit in till Datainspektionen senast tre veckor från den dag beslutet meddelades för att kunna prövas. Datainspektionen sänder överklagandet vidare till Förvaltningsrätten i Stockholm för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Ingela Alverfors

Kopia till:
Personuppgiftsombudet