

Socialnämnden
Nacka Kommun
131 81 Nacka

Beslut efter tillsyn enligt personuppgiftslagen (1998:204)

Datainspektionens beslut

Datainspektionen konstaterar att Socialnämnden i Nacka kommun har behandlat känsliga personuppgifter i sitt e-postsystem utan att vidta tillräckliga säkerhetsåtgärder enligt 31 § personuppgiftslagen.

Datainspektionen förelägger Socialnämnden i Nacka kommun att krypterings-skydda känsliga personuppgifter när de kommuniceras över ett öppet nät samt att vidta tekniska åtgärder för att säkerställa att endast den tänkta mottagaren kan ta del av uppgifterna.

Med detta avslutar Datainspektionen ärendet. Ärendet kan komma att följas upp.

Redogörelse för tillsynsärendet

Datainspektionen har genom en nyhetsartikel i Nacka Värmdö Posten uppmärksammat på att ett e-postmeddelande skickats från handikapp-, psykiatri- och beroendeenheten innehållande bland annat känsliga personuppgifter.

Socialnämnden i Nacka kommun är personuppgiftsansvarig för behandling av personuppgifter vid handikapp-, psykiatri- och beroendeenheten.

Datainspektionen har inlett tillsyn och Socialnämnden har yttrat sig.

Nämnden har i sitt yttrande i huvudsak anfört följande.

Ett brev har som bilaga till ett e-postmeddelande skickats till ett barns förälder på uttrycklig begäran av föräldern. Vid framtagandet av brevet återanvändes ett äldre elektroniskt dokument som mall, där de äldre uppgifterna ersattes med det aktuella barnets. Genom en funktion i ordbehandlingsprogrammet kunde den mottagande föräldern ta del av de äldre uppgifterna, som rörde ett annat barn.

Socialnämnden har som rutin att inte skicka brev per e-post. Denna rutin är inte formaliserad i ett formellt beslut. Det har emellertid varit ett naturligt arbetssätt med hänsyn till sekretess och kraven på personuppgiftsbehandling, särskilt då vid behandling av känsliga personuppgifter. Ett avsteg från dessa rutiner borde inte ha skett, men gjordes på uttrycklig begäran av e-postmeddelandets mottagare. Socialnämnden har inte för avsikt att kommunicera känsliga personuppgifter i öppna nät, såsom via e-postsystem. Om ett brev i något läge måste skickas via e-post skall det i så fall skannas in så att äldre uppgifter inte kan tas fram. Stor noggrannhet skall i så fall råda så att misstag inte uppstår vid angivande av mottagande e-postadress. Som rutin måste också gälla att brev och skrivelser alltid skrivs i ett nytt dokument. Socialnämnden ser mycket allvarligt på det inträffade. Kommunen arbetar på centrala direktiv för hur skrivelser skall kunna skickas i e-postsystem.

Skäl för beslutet

Enligt 31 § personuppgiftslagen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, kostnaden för åtgärderna, särskilda risker med behandlingen och hur pass känsliga uppgifterna är.

I Datainspektionens Allmänna råd ”Säkerhet för personuppgifter” nämns uppgifter angående ekonomisk hjälp eller vård inom socialtjänsten som exempel på personuppgifter som normalt är att anse som känsliga.

Vid bedömning av hur pass känsliga uppgifterna hos socialtjänsten är ska särskilt beaktas om personuppgifterna definieras som känsliga i personuppgiftslagen, om de omfattas av tystnadsplikt eller sekretess enligt sekretesslagen (1980:100) eller annan lagstiftning samt om de är att anse som ömtåliga enligt lagen om behandling av personuppgifter inom socialtjänsten (2001:454).

Känsliga uppgifter enligt 13 § personuppgiftslagen får endast lämnas ut via öppna nät till identifierade användare vars identitet är säkerställd med en teknisk funktion som kryptering, engångslösenord eller motsvarande. Känsliga personuppgifter ska dessutom vid överföring via öppet nät, till exempel Internet, föras med krypteringsskydd.

Den aktuella behandlingen har skett i strid mot 31 § personuppgiftslagen genom att känsliga personuppgifter kommunicerats oskyddat över öppet nät och utan att åtgärder vidtagits för att säkerställa mottagarens identitet.

För att säkerställa att personuppgifter i fortsättningen kommuniceras med fullgod säkerhet bör socialnämnden med stöd av 32 § personuppgiftslagen föreläggas att krypteringsskydda känsliga personuppgifter när de kommuniceras över ett öppet nät samt att vidta tekniska åtgärder för att säkerställa att endast den tänkta mottagaren kan ta del av uppgifterna.

Övrigt

Datainspektionen förutsätter att de i Socialnämndens yttrande åberopade centrala direktiven för hur skrivelser skall kunna skickas i e-postsystem, utformas med beaktande av detta beslut.

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 Länsrätten i Stockholms län för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Detta beslut har fattats av generaldirektören Göran Gräslund i närvaro av datarådet Katja Isberg Amnäs och IT-säkerhetsspecialisten Magnus Bergström, föredragande.

Göran Gräslund

Magnus Bergström

Kopia till:

Personuppgiftsombudet Hans-Ivar Swärd, Nacka Kommun, 131 81 Nacka