JURIDISKA aspekter

Chatta med socialtjänsten



# Innehållsförteckning

[Tillgänglighet via elektroniska kommunikationsformer 3](#_Toc391370114)

[Skyldighet att skydda känsliga personuppgifter 3](#_Toc391370115)

[Kommunikation av övriga personuppgifter](#_Toc391370117) 3

[Hantering av inkommande handling 4](#_Toc391370118)

[Specifika förutsättningar för olika kommunikationsmedel 4](#_Toc391370118)

[E-post 5](#_Toc391370118)

[SMS 5](#_Toc391370118)

[Chatt 6](#_Toc391370118)

[Chattlogg 7](#_Toc391370118)

[Utlämnande av allmän handling 8](#_Toc391370118)

**Tillgänglighet via elektroniska kommunikationsformer**

Socialtjänsten har, liksom andra myndigheter, enligt 5 § förvaltningslagen (1986:223), FL ett generellt ansvar att möjliggöra en kontakt för enskilda via e-post och lämna svar på samma sätt.

Till den omarbetning av förvaltningslagen som har föreslagits (SOU 2010:29) så lyfts även fram att myndigheterna på lämpligt sätt ska informera allmänheten om den e-postadress (eller annat elektroniskt mottagningsställe) till vilken meddelanden kan sändas. I den nya förvaltningslagen föreslås också att myndigheten ska se till att kontakterna med enskilda blir smidiga och enkla och det understryks också i SOU-rapporten att tillgänglighet via e-post är ett minimikrav vad gäller elektroniska kommunikationsformer.

**Skyldighet att skydda känsliga personuppgifter**

I 31 § personuppgiftslagen (1998:204), PuL, föreskrivs att den personuppgiftsansvarige, vilket inom kommunerna är ansvarig nämnd, är skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Som personuppgifter definieras enligt 3 § PuL all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Omfattningen på skyddsåtgärderna är bland annat beroende av om personuppgifterna bedöms vara känsliga eller inte. Som känsliga personuppgifter räknas enligt 13 § PuL samt Datainspektionens allmänna råd ”Säkerhet för personuppgifter” (2008) bland annat uppgifter som avslöjar en enskilds ekonomiska eller personliga situation, hälsa, sexualliv, etniskt ursprung, politiska åsikter och religiös övertygelse. Personuppgifter om ekonomisk hjälp och vård inom socialtjänsten eller lagöverträdelser som innefattar brott och domar i brottmål klassificeras inte som känsliga uppgifter enligt personuppgiftslagen men bör enligt Datainspektionen (2008) ändå jämställas med känsliga personuppgifter. I praktiken innebär detta att elektronisk kommunikation (e-post, webb-formulär, chatt, sms etc.) som innehåller känsliga personuppgifter måste krypteras på ett sådant sätt att endast den avsedda mottagaren kan ta del av dem (Datainspektionen, 2007). De tekniska förutsättningarna för att göra detta redogörs för nedan under respektive kommunikationsform.

**Kommunikation av övriga personuppgifter**

När det gäller kommunikation av personuppgifter som inte bedöms vara känsliga, vilket till exempel kan handla om påminnelser, boka eller ändra mötestider samt andra enklare typer av icke integritetskänslig information så finns inte samma krav på kryptering. Däremot behövs ett medgivande från klienten till att uppgifter kommuniceras i denna form (SOSFS 2008:14 2 kap 5 § Datainspektionen, 2011). Ett dylikt medgivande kan till exempel inhämtas vid ett första fysiskt möte. Ett medgivande anses också ha givits om en sökande själv kontaktar en myndighet per e-post, sms eller via annan elektronisk kommunikationskanal och ber om uppgifter. Datainspektionen betonar dock att ett beslut om att skicka påminnelser via öppna nät alltid ska föregås av en risk- och sårbarhetsanalys för att säkerställa att individens integritet inte kränks och att sekretess eller tystnadsplikten inte åsidosätts.

Eventuellt kan det finnas behov av att radera klientens ursprungliga fråga i svaret då den kan innehålla känslig information. Svaret bör även vara formulerat i generella ordalag. Information om att en person står i kontakt med socialtjänsten anses inte nödvändigtvis vara att räkna som känsliga uppgifter utan det är innehållet i kommunikationen som är det avgörande.

Ett medgivande från klienten kan dock aldrig möjliggöra att känsliga personuppgifter skickas oskyddade. Trots att frågan ställts på elektronisk väg är det i de fall där känsliga personuppgifter ska kommuniceras nödvändigt att istället välja en annan säker kommunikationsväg, som till exempel telefon, brev eller ett fysiskt möte, om det inte är möjligt att kryptera svaret på elektronisk väg (Datainspektionen, 2011).

**Hantering av inkommande handlingar**

All skriftlig kommunikation till och från en myndighet innebär vanligtvis att allmänna handlingar uppstår. Digital kommunikation som till exempel chatt, e-post eller sms är inget undantag. Varje medborgare har enligt 2 kap tryckfrihetsförordningen (1949:105), TF, rätt att ta del av myndigheters allmänna handlingar dock med vissa undantag som regleras i 3-4 §§ 5 kap offentlighets- och sekretesslagen (2009:400), OSL. Enligt 1 § 5 kap OSL ska allmänna handlingar vanligtvis registreras så fort de har inkommit till myndigheten. Vid osäkerhet kring vad som är allmänna handingar eller hanteringen av dessa så bör förvaltnings registrator eller arkivarie rådfrågas.

Handlingar som är av ringa betydelse behöver inte registreras om de kan hållas ordnade på annat sätt och det tydligt framgår att och när de har inkommit. Detta är till exempel är fallet i många sociala medier. Handlingar av ringa betydelse kan gallras vid inaktualitet enligt kommunens dokumenthanteringsplan. Gallring vid inaktualitet innebär att handlingarna ska raderas så fort de inte längre behövs. Vid osäkerhet kring gallring av allmänna handlingar ska därför alltid förvaltningens arkivarie kontaktas.

Ytterligare ett undantag från skyldigheten att registrera allmänna handlingar gäller handlingar som hör till enskildas personakter inom socialtjänsten. Dessa ska istället överföras till den aktuella akten (§ 2 Offentlighets- och sekretess-förordningen).

Eftersom kommunen fortfarande har ett pappersbaserat diarium ska elektroniska handlingar som innehåller känsliga uppgifter och/eller sekretess (men inte tillhör en enskild personakt enligt ovan) skrivas ut för att sparas i pappersform, diarieföras och därefter raderas från telefonen, e-postprogrammet, det sociala mediet eller datorn. Uppgifter som ligger kvar på datorn är visserligen skyddade genom kryptering, men risken för att meddelandet kan spridas till exempel genom att handläggaren av misstag vidarebefordrar det bedöms vara tillräckligt stor för att istället rekommendera att meddelandet istället raderas.

**Specifika förutsättningar för olika kommunikationsmedel**

E-post

Som framgår av texten ovan finns det inget generellt förbud mot att skicka e-post till klienter. Allmänt hållna e-postmeddelanden som inte innehåller känsliga personuppgifter går bra att skicka under förutsättning att klienten har givit sitt medgivande.

När det gäller känsliga personuppgifter så ställer personuppgiftslagen, som nämnts ovan, krav på säkerheten vid kommunikationen. Detta innebär att e-post innehållande dylik information måste krypteras så att endast den avsedda mottagaren kan ta del av dem.

Om det är möjligt att i generella ordalag svara på en fråga, som inkommit via e-post och innehåller känsliga personuppgifter eller sekretess, så kan svaret också skickas med e-post. Det är dock viktigt att radera originalmeddelandet från klienten så att inte det följer med svaret. Svaret ska, om det inte tillhör en enskild personakt eller är av ringa betydelse, diarieföras tillsammans med det ursprungliga meddelandet innehållandes den ursprungliga frågan.

**Sms**

Kommunikation via sms lyder under samma lagstiftning som e-post och annan elektronisk kommunikation. Det finns idag ingen möjlighet att kryptera utgående sms och inga känsliga personuppgifter kan därmed kommuniceras den vägen. Påminnelser eller andra typer av allmänt hållna sms som inte innehåller känsliga personuppgifter går bra att skicka under förutsättning att det finns ett medgivande från klienten. Om klienten sms:ar till socialtjänsten likställs det med ett medgivande och svar kan därmed lämnas på samma sätt under förutsättning att inga känsliga uppgifter lämnas ut.

Både inkommande och utgående sms är allmänna handlingar i och med att de också innebär skriftlig kommunikation till eller från en myndighet. Inkommande sms som innehåller känsliga personuppgifter ska således föras över till datorn, skrivas ut och diarieföras alternativt överföras till aktuell personakt och därefter raderas från telefonen. Hur sms förs över från telefonen till datorn ser olika ut på olika telefoner. På äldre telefoner görs överföringen ofta genom att telefonen kopplas ihop med datorn med usb-kabel. På nyare telefoner kan meddelanden antingen vidarebefordras till en mejladress eller så kan en skärmdump (ögonblicksbild) tas över sms-konversationen. Om programvaran för att föra över sms till datorn inte finns ska sms:en istället skrivas av manuellt (SKL, 2009).

**Chatt**

En chatt är ett digitalt skriftligt samtal som sker i realtid. En avslutad chatt genererar ofta vad som brukar kallas för en chatt-logg, vilket i likhet med inkommande och utgående e-post och sms vanligtvis är en allmän handling som ska hanteras på motsvarande sätt. De tekniska och juridiska förutsättningarna för detta beror dock på vilken typ av chatt som används.

Som nämnts ovan är det dock viktigt att hantera de chatt-loggar som skapas på lämpligt sätt utifrån vilken typ av allmänna handlingar de är.

När det gäller kommunikation via chatt med klienter inom socialtjänsten som inte är anonyma utan kända sedan tidigare så uppstår ett behov av att verifiera mottagaren. Om det inte går att säkerställa att medborgaren/klienten är den som den utger sig för att vara kan socialtjänsten endast besvara chatten i allmänna ordalag och ge generella råd. Socialtjänsten kan däremot aldrig uttala sig om en klients personliga förhållanden om identiteten inte är säkerställd.

I den projekterade chatten finns det i dagsläget ingen möjlighet för klienten att logga in med e-legitimation för att på så sätt verifiera sin identitet. Möjliga andra lösningar för att verifiera klientens identitet skulle dock kunna vara att använda en webb-kamera (om klienten är känd till utseendet) eventuellt i kombination med att den anställda kommer överens om ett kodord med klienten eller ber klienten återberätta det senaste samtalet så att den på detta sätt kan identifieras.

Det är svårt att komma med generella råd i denna fråga då det varken finns praxis eller någon form av styrande dokument. Det viktiga för socialtjänsten är dock att med lämpliga metoder säkerställa att det verkligen är rätt person som de pratar med, precis som vid ett telefonsamtal med en klient. Metoderna för att säkerställa identiteten kan komma att variera beroende på vilken kontakt som socialtjänsten tidigare har haft med klienten.

*Chattloggen*

Kommunen har valt att spara chattloggen hos leverantören. Loggen sparas, enligt med kommunens dokumenthanteringsplan i tre månader och gallras sedan.

Chatten ska vara anonym och innehåller således inga personuppgifter. Blir det ändock så att personuppgifter eller andra känsliga uppgifter framkommer under chatten så tar kommunen hem loggen och tillser att den gallras hos leverantören. Loggen registreras istället hos kommunen.

*Utlämnande av allmän handling*

All skriftlig kommunikation med myndigheten innebär att en allmän handling uppstår. Elektronisk kommunikation såsom e-post, sms och chatt är inget undantag.

Allmänhetens rätt att ta del av dessa allmänna handlingar hanteras i enlighet med bestämmelserna i tryckfrihetsförordningens 2 kap 2 §.

Beslut att inte lämna allmänhandling är delegerat till socialchef

