Sveriges Kommuner och Regioner SKR
Ert ärende 20/00618

Svar på förfrågan från Sveriges Kommuner och Regioner (SKR)

Datainspektionen har den 15 april 2020 mottagit en förfrågan från Sveriges Kommuner och Regioner (SKR).

Förutom till SKR skickar Datainspektionen en kopia av detta svar till Socialdepartementet.

Sammanfattning

Ett strukturerat arbetssätt för att analysera både risker med behandlingen av personuppgifter och vad som kännetecknar behandlingen (art, sammanhang osv.) är viktiga beståndsdelar för att den personuppgiftsansvarige ska kunna avgöra vilka säkerhetsåtgärder (organisatoriska och tekniska) som behövs.

Analysarbete, slutsatser och vidtagna säkerhetsåtgärder behöver den personuppgiftsansvarige dokumentera som ett led i ansvarsskyldigheten för att kunna visa att dataskyddsreglerna efterlevs.

Datainspektionen kan lagligen varken efterge ansvarsskyldigheten eller till socialtjänsten rekommendera att den använder sig av något visst slag av it-stöd.

SKR:s frågeställning

Kortfattat anför SKR att verksamhetsutövare inom socialtjänsten behöver vägledning för sin tolkning av artikel 32 dataskyddsförordningen och därmed den närmare innebörden av artikel 5.1. f. SKR:s fråga är om det finns utrymme i dataskyddslagstiftningen för socialtjänsten att under

rådande extraordinära omständigheter använda sig av digitala mötestjänster för att fullgöra sitt uppdrag, trots att de inte i alla delar erbjuder ett lämpligt skydd för känsliga personuppgifter, t.ex. stark autentisering. Vägledning önskas också om vilka andra medel som står till buds för att hantera socialtjänstens dilemma. Skälen är följande. På grund av coronaviruset har socialtjänsten till stor del ersatt fysiska möten med digitala möten. För detta syfte används både kostnadsfria och kommersiella videolösningar. SKR har emellertid erfarit att dessa videotjänster inte alltid ger ett adekvat skydd för enskildas personuppgifter inom socialtjänsten som i många fall är av känslig natur. Flertalet videotjänster saknar stark autentisering (tvåfaktorsutentisering) och erbjuder inte heller alla gånger ett adekvat skydd för själva överföringen av personuppgifter över internet. Nationella och säkra videolösningar som är skräddarsydda för socialtjänstens behov saknas i dagsläget.

Datainspektionens vägledning

Datainspektionen informerar om följande.

Den som är personuppgiftsansvarig har ansvarsskyldighet och ska kunna visa att de grundläggande dataskyddsprinciperna efterlevs, artikel 5.2 dataskyddsförordningen. Inom socialtjänsten är kommunal myndighet eller juridisk eller fysisk person som ansvarar för privat verksamhet personuppgiftsansvarig enligt 11 och 17 §§ förordningen om behandling av personuppgifter inom socialtjänsten (2001:637). Det finns inte något stöd i dataskyddsförordningen eller i nationell rätt som medger att Datainspektionen efterger ansvarsskyldigheten.

Oavsett vilket it-stöd som används när socialtjänsten utför sina uppgifter måste den se till att de personuppuppgifter som behandlas är adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas, uppgiftsminimering enligt artikel 5.1 c dataskyddsförordningen. Vidare gäller kravet på att behandlingen är nödvändig för att exempelvis utföra en uppgift av allmänt intresse, artikel 6.1 c och e. När det gäller artikel 6.2 och 6.3 om nationell rätt finns kompletterande nationell rätt genom främst lagen (2001:454) och förordningen om behandling av personuppgifter inom socialtjänsten. Enligt 6 § tredje stycket lagen om behandling av personuppgifter inom socialtjänsten har en registrerad person inte rätt att motsätta sig sådan behandling av uppgifter som är tillåten enligt den lagen. Sammantaget innebär nämnda bestämmelser att den personuppgiftsansvarige behöver se till att behandlingen av personuppgifterna är proportionerlig, oavsett vilket it-stöd man använder.

SKR:s frågeställning fokuserar på säkerhetsåtgärder. Datainspektionen vill framhålla att det är den personuppgiftsansvarige som ska se till att personuppgifterna behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder, integritet och konfidentialitet artikel 5.1 f dataskyddsförordningen. Av artikel 32.1 och 32.2 framgår vilket närmare analysarbete en personuppgiftsansvarig måste göra när det gäller att bedöma lämplig säkerhetsnivå för att kunna bestämma vilka säkerhetsåtgärder som ska vidtas. Artiklarna lyder.

Artikel 32
Säkerhet i samband med behandlingen
1. Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt

a) pseudonymisering och kryptering av personuppgifter,
b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,
c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,
d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

2. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Med den senaste utvecklingen avses att den senast tillgängliga teknologin ska beaktas. Det innebär att den personuppgiftsansvarige måste ha både kunskap och hålla sig uppdaterad om den teknologiska utvecklingen.

Med genomförandekostnaderna avses att personuppgiftsansvarig kan beakta kostnaden för implementation och kontinuerligt underhåll för ett effektivt införande av samtliga dataskyddsprinciper genom hela processen.

Datainspektionen anser att beaktande av behandlingens art, omfattning, sammanhang och ändamål är att uppfattas som ett krav på den personuppgiftsansvarige att genomlysa och analysera behandlingens alla relevanta omständigheter utifrån på vilka områden inom socialtjänsten man vill använda ett visst digitalt stöd och varför. Även om uppräkningen art,

omfattning, sammanhang och ändamål kan vara överlappande, är det viktigt att den personuppgiftsansvarige analyserar alla relevanta omständigheter för att balansera dessa i förhållande till riskerna.

När det gäller art, omfattning, sammanhang och ändamål kan följande vara ett sätt att tänka, men på intet sätt uttömmande. Behandling hos socialtjänsten omfattar insamling och annan behandling personuppgifter i olika slag av verksamheter inom socialtjänsten, 2 § lagen om behandling av personuppgifter inom socialtjänsten. I vilka verksamheter inom socialtjänsten kan användning av videotjänster vara aktuell och varför? I vilken omfattning? Är det olika slags tjänster som behöver genomlysas? Är behandlingen i enlighet med angivna ändamål för behandlingen av personuppgifterna i förordningen om behandling av personuppgifter inom socialtjänsten? Behandling inom socialtjänsten kan omfatta känsliga personuppgifter, troligen främst hälsa, och andra ömtåliga personuppgifter om familjeförhållanden och ekonomi. Kommer de slagen av personuppgifter att överföras och samlas in via videotjänster? Det är viktigt att behandlingen är proportionerlig, dvs. hur sker exempelvis uppgiftsminimering vid personuppgifternas överföring och insamling via en videotjänst? En enskild person som har kontakt med socialtjänsten får anses ha en hög förväntan på att obehöriga inte ska kunna ta del av uppgifterna, bl.a. för att det finns bestämmelser om tystnadsplikt. Barns personuppgifter förtjänar särskilt skydd, eftersom barn kan vara mindre medvetna om berörda risker, följder och skyddsåtgärder samt om sina rättigheter när det gäller behandling av personuppgifter, skäl 38 till dataskyddsförordningen. Vad betyder i sammanhanget enskildas förväntningar på skyddet mot obehöriga och skyddet för barns personuppgifter?

När det gäller risker ska den personuppgiftsansvariga analysera de risker som kan uppstå och riskernas varierande sannolikhetsgrad och allvar. Det finns flera olika sätt att analysera risk, exempelvis genom en riskanalys där hot och oönskade händelser identifieras som kan leda till negativa konsekvenser. Genom en riskanalys får den personuppgiftsansvarige ett underlag för att ta beslut om vilka säkerhetsåtgärder som ska införas. Nästa skede kan vara att genomföra en gapanalys för att balansera säkerhetsåtgärderna mot säkerhetsbehoven där syftet är att identifiera den önskvärda nivån på informationssäkerheten och den faktiska nivån för att överbrygga gapet. Som ett stöd i arbetet finns ett flertal vedertagna standarder, metoder och vägledningar att utgå ifrån.

Sammanfattningsvis är ett strukturerat arbetssätt för att analysera både risker med behandlingen av personuppgifter inom socialtjänsten och vad som kännetecknar den (art, sammanhang osv.) viktiga beståndsdelar för att

den personuppgiftsansvarige ska kunna avgöra vilka säkerhetsåtgärder (organisatoriska och tekniska) som behöver vidtas oavsett teknik för digital hantering. Sådant analysarbete, slutsatser och vidtagna säkerhetsåtgärder i enlighet med artikel 32 dataskyddsförordningen bör den personuppgiftsansvarige dokumentera som ett led i att kunna visa att dataskyddsreglerna efterlevs. Inom socialtjänsten – som ofta hanterar känsliga och andra ömtåliga personuppgifter – anser Datainspektionen att det är särskilt viktigt att det finns en förmåga att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och –tjänsterna.

Eftersom den personuppgiftsansvarige har ett ansvar att visa att dataskyddsprinciperna efterlevs behöver analysarbete, slutsatser och vidtagna säkerhetsåtgärder gällande artikel 32 dataskyddsförordningen dokumenteras av den personuppgiftsansvarige, jfr. artikel 5.1 f och 5.2.

Det kan tilläggas att den personuppgiftsansvarige behöver ha rutiner för att upptäcka och åtgärda incidenter som rör personuppgifter, vilket är innebörden av artikel 33.5. dataskyddsförordningen. Den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter, oavsett om incidenten ska anmälas till Datainspektionen eller inte, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Denna dokumentation ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden.

Övrigt

SKR uppger följande. I en hemställan den 23 mars 2020 till regeringen har SKR begärt ett antal omedelbara behov av regelförändringar eller undantag från gällande regelverk för att underlätta och effektivisera kommunernas arbete med att hantera effekterna av det nya coronaviruset. I hemställan föreslår SKR att regeringen ska besluta om undantag i gällande författningar för att kunna erbjuda möten med invånaren både på dator och mobil, trots att säker inloggning saknas och utan risk för administrativa sanktionsavgifter. Vidare uppger SKR att som ett led i beredningen av hemställan har regeringen emellertid uppmanat SKR att först uttömma möjligheten att söka samråd med Datainspektionen i egenskap av tillsynsmyndighet för att sondera förutsättningarna om det finns utrymme i dataskyddslagstiftningen för socialtjänsten att under rådande extraordinära omständigheter använda sig av digitala mötestjänster, trots att de inte i alla delar erbjuder ett adekvat skydd för känsliga personuppgifter, t.ex. stark autentisering.

Datainspektionen skickar en kopia av detta svar till Socialdepartementet.

Detta svar har beslutats av enhetschefen Malin Blixt efter föredragning av avdelningsdirektören Suzanne Isberg. I den slutliga handläggningen har även medverkat it-säkerhetsspecialisten Johan Ma.

Malin Blixt, 2020-04-21 (Det här är en elektronisk signatur)