Integritetsskydds myndigheten

Integritetsskyddsmyndighetens kontroll av behandling av uppgifter om vårdsökande i samband med samtal till 1177 – en rapport

Diarienummer:
DI-2021-5220

Datum:
2021-06-07

Innehåll

Bakgrund ... 1
Inledning ... 3
Vad är 1177 Vårdguiden? ... 3
Incidenten – oskyddad exponering av ljudfiler från telefonsamtal till 1177 ... 3
Aktörer som omfattades av tillsyn ... 4
Roller och kraven på säkerhet ... 4
Generellt om ansvarsförhållandet mellan personuppgiftsansvarig och biträde ... 4
Ansvarsfrågor enligt dataskyddsförordningen och krav på säkerhet ... 5
Krav på öppenhet och information om vem som är personuppgiftsansvarig ... 6
Tillsynsobjektens roller och ansvar och förhållandet dem emellan ... 8
Översiktlig beskrivning av informationsflödet ... 8
Regionernas roller och ansvar ... 9
Regionerna Sörmland och Värmland ... 9
Region Stockholm ... 9
Ineras roll och ansvar ... 10
MedHelps roll och ansvar ... 10
Voice's roll och ansvar ... 12

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

Bakgrund

Den 18 februari 2019 uppmärksammades att en stor mängd samtal till numret 1177 gjorts tillgängliga på en webbserver då Computer Sweden publicerade en artikel med rubriken ”2,7 miljoner inspelade samtal till 1177 helt oskyddade på internet”.[1]

I artikeln beskrevs hur man kunde ta del av inspelade samtal till rådgivningsnumret 1177 på en server utan lösenordsskydd eller annan säkerhet.

Rapporteringen följdes av att ett antal anmälningar av personuppgiftsincidenter gjordes till Integritetsskyddsmyndigheten (IMY), tidigare Datainspektionen.[2] Personuppgiftsincidenter – säkerhetsincidenter där personuppgifter t.ex. ändrats, gått förlorade eller kommit i orätta händer – ska anmälas av den personuppgiftsansvariga till IMY om incidenten kan medföra en risk för människors friheter och rättigheter.

Anmälningar om personuppgiftsincidenter inkom bl.a. från företagen Voice Integrate Nordic AB (Voice),[3] MedHelp AB (MedHelp)[4] och MediCall Co Ltd (MediCall).[5]

Artikeln och inkomna anmälningar av personuppgiftsincidenter ledde till att IMY inledde tillsyn mot sex aktörer som kunde kopplas till incidenten eller sjukvårdsrådgivning via telefonnumret 1177; Voice, MedHelp, Inera AB (Inera), samt regionerna Stockholm, Värmland och Sörmland. Under IMY:s granskning har regionerna Värmland och Sörmland upphört med att anlita MedHelp som vårdgivare för att besvara samtal till 1177.

Syftet med dessa granskningar var att kontrollera aktörernas koppling till sjukvårdsrådgivning via telefonnumret 1177, vem som var personuppgiftsansvarig eller personuppgiftsbiträde och hur dessa levt upp till sina respektive skyldigheter enligt dataskyddsförordningen[6] och nationell kompletterande rätt inom hälso- och sjukvårdsområdet avseende säkerhet och enskilda vårdsökandes rätt till information.

I denna rapport beskrivs dessa tillsynsärenden och sambandet mellan de olika verksamheternas roller och ansvar översiktligt. För mer ingående information finns tillsynsbesluten på IMY:s webbplats.[7]

Rapporten redovisar förhållandena under IMY:s granskning.

IMY inledde inte tillsyn mot MediCall eftersom MediCall är ett thailändskt bolag med verksamhet i Thailand och utan företrädare inom EU.

[1] https://computersweden.idg.se/2.2683/1.714787/inspelade-samtal-1177-vardguiden-oskyddade-internet
[2] Datainspektionen bytte den 1 januari 2021 namn till Integritetsskyddsmyndigheten.
[3] IMY:s ärende PUI-2019-705.
[4] IMY:s ärende PUI-2019-689.
[5] IMY:s ärende PUI-2019-698.
[6] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[7] https://www.imy.se/om-oss/arbetssatt/tillsyn/tillsynsbeslut/

Inledning

Vad är 1177 Vårdguiden?

1177 Vårdguiden är en sjukvårdstjänst som erbjuds och drivs gemensamt av alla Sveriges 21 regioner. Tjänsten är en samlingsplats för information om vård och hälsa och som kan nås både via webben och telefon. Telefonnumret 1177 är ett nationellt telefonnummer för sjukvårdsrådgivning dit man kan ringa för att få råd och vägledning av sjuksköterskor.[8]

1177 Vårdguiden är inte en enskild aktör, utan varje region bedriver sin egen verksamhet för sjukvårdsrådgivning, antingen i egen regi eller genom underleverantörer. För att hålla samma kvalitet ingår regionerna i ”ett nationellt nätverk med ett gemensamt arbetssätt”.[9]

På webbplatsen 1177.se informeras besökaren om att *alla samtal spelas in och att rådgivningssamtal journalförs. Vidare informeras om att det är respektive vårdgivare som ansvarar för behandlingen av personuppgifter i journaler och att personuppgifter hanteras korrekt och lagligt.*

Incidenten – oskyddad exponering av ljudfiler från telefonsamtal till 1177

I personuppgiftsanmälningarna beskrevs incidenten som obehörig åtkomst där personer utanför organisationen, som saknat behörighet, tagit del av känsliga personuppgifter bl.a. om patienters hälsa. Orsaken uppgavs vara ett säkerhetshål[10] och intrång[11] i Voice server, Voice NAS, som medfört att känsliga personuppgifter i form av ljudfiler med samtal till 1177 hade exponerats mot internet utan några skyddsmekanismer.[12]

Syftet med servern Voice NAS var initialt att hantera och lagra Voice interna filer. Den var passiv och saknade inloggningskonton då den var avsedd att användas för Voice egna ändamål inifrån det egna nätverket.

Incidenten berodde på att Voice NAS, genom en felkonfigurering, kunde nås utanför systemet via ett säkerhetshål i programvaran som medförde att servern tillät okrypterad kommunikation. Till följd av det blev en stor mängd samtal åtkomliga utan lösenordsskydd eller annan säkerhet för alla med en internetuppkoppling. Det som krävdes för att få tillgång till samtalsfilerna var IP-adressen till servern.

Det fanns per den 18 februari 2019 ca 2,7 miljoner filer på servern. Ett samtal motsvarar i genomsnitt ca tre till fyra filer, men kan utgöra upp till tio filer. IMY har uppskattat antalet lagrade samtal till mellan 650 000 och 900 000.

Voice stängde ned lagringsservern Voice NAS den 18 februari 2019 så att den inte längre var nåbar via internet. Det har inte kunnat fastställas när felkonfigureringen ägde rum eller under hur lång tid filerna var exponerade.

---

[8] https://www.1177.se/Stockholm/om-1177-vardguiden/1177-vardguiden-pa-telefon/om-1177-vardguiden-pa-telefon/.
[9] https://www.1177.se/Stockholm/om-1177-vardguiden/1177-vardguiden-pa-telefon/om-1177-vardguiden-pa-telefon/.
[10] IMY:s ärende PUI-2019-705.
[11] IMY:s ärende PUI-2019-698.
[12] IMY:s ärende PUI-2019-698.

Aktörer som omfattades av tillsyn

I de anmälningar av personuppgiftsincidenter som inkom från företagen Voice och MedHelp uppgav de sig vara personuppgiftsansvariga. I anmälningarna uppgavs vidare att incidenten var av betydande allvarlighet, att den berott på den mänskliga faktorn samt att företagen fått kännedom om incidenten via information från artikeln i Computer Sweden eller Inera AB. Tillsyn inleddes mot båda företagen.

Tillsyn inleddes också mot Inera mot bakgrund av artikeln och informationen på Ineras webbplats om att Inera förvaltar och utvecklar de gemensamma systemen för 1177 på telefon som regionerna behöver i sin verksamhet.

Både MedHelp och Inera uppgav att de agerade på uppdrag av regionerna Stockholm, Värmland och Sörmland som de hade avtal med. Tillsyn inleddes mot den bakgrunden även mot de tre regionerna.

Roller och kraven på säkerhet

Generellt om ansvarsförhållandet mellan personuppgiftsansvarig och biträde

Tydliga ansvarsförhållanden är avgörande för ett fullgott dataskydd.

Det är den som är personuppgiftsansvarig som ska göra anmälan när det skett en personuppgiftsincident. Att flera anmälningar inkom till IMY tyder på oklara förhållanden kring vem som var personuppgiftsansvarig för behandlingen av personuppgifterna i ljudfilerna. Personuppgiftbiträdets roll när det gäller personuppgiftsincidenter är att utan onödigt dröjsmål underrätta den personuppgiftsansvarige om en inträffad personuppgiftsincident.

Den som är personuppgiftsansvarig ska vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att förhindra obehörigt röjande av eller obehörig åtkomst till uppgifter. Som personuppgiftsansvarig måste man också skriva ett avtal med det personuppgiftsbiträde man anlitar. Men även personuppgiftsbiträden har en skyldighet att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att förhindra obehörigt röjande av eller obehörig åtkomst till uppgifterna.

Dessutom måste organisationer som behandlar personuppgifter ha en grundläggande it-säkerhet, oavsett om man hanterar känsliga vårduppgifter eller inte.

Även om själva hanteringen av personuppgifter sker hos ett personuppgiftsbiträde är det alltid den som är personuppgiftsansvarig som är ytterst ansvarig för de personuppgifter som hanteras. Det gäller bland annat att behandlingen av personuppgifterna är laglig, att de registrerade får information om behandlingen av personuppgifterna och att det vidtas lämpliga säkerhetsåtgärder.

Utöver det har ett personuppgiftsbiträde egna skyldigheter att vidta lämpliga och tillräckliga säkerhetsåtgärder för att skydda de personuppgifter som hanteras på uppdrag av den personuppgiftsansvariga.

När det gäller skyddsvärda eller integritetskänsliga personuppgifter är det särskilt viktigt att det finns förmåga, rutiner och tekniska lösningar på plats som säkerställer att uppgifterna inte blir åtkomliga för de som inte ska ha tillgång till dem. Det gäller både den som är personuppgiftsansvarig och personuppgiftsbiträden.

Om flera aktörer är inblandade får det inte råda tvivel, delade meningar eller oklarheter om vem som är personuppgiftsansvarig, vem som är personuppgiftsbiträde, och vilket ansvar respektive vilka skyldigheter var och en har. Förhållandet mellan personuppgiftsansvarig och personuppgiftsbiträde ska enligt artikel 28 i dataskyddsförordningen regleras i ett avtal och biträdet får bara behandla personuppgifter på den ansvariges dokumenterade instruktioner.

Ansvarsfrågor enligt dataskyddsförordningen och krav på säkerhet

Dataskyddsförordningen infördes den 25 maj 2018 och är den primära rättsliga regleringen vid behandling av personuppgifter. Detta gäller även vid behandling av personuppgifter inom hälso- och sjukvården.

De grundläggande principerna för behandling av personuppgifter anges i artikel 5 i dataskyddsförordningen. En grundläggande princip är kravet på säkerhet enligt artikel 5.1 f, som anger att personuppgifterna ska 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. Av artikel 5.2 framgår den s.k. ansvarsskyldigheten, dvs. att den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna i punkt 1 efterlevs.

Artikel 24 handlar om den personuppgiftsansvariges ansvar. Av artikel 24.1 framgår att den personuppgiftsansvarige ansvarar för att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen. Åtgärderna ska genomföras med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers fri- och rättigheter. Åtgärderna ska ses över och uppdateras vid behov.

Artikel 32 reglerar säkerheten i samband med behandlingen och anger även personuppgiftsbiträdes ansvar att vidta säkerhetsåtgärder för att skydda personuppgifterna. Enligt punkt 1 ska den personuppgiftsansvarige och personuppgiftsbiträdet 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 vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken (…). Enligt punkt 2 ska vid bedömningen av lämplig säkerhetsnivå särskild hänsyn tas till de risker som behandlingen medför, i synnerhet från oavsiktlig eller olaglig förstöring.[13]

Personuppgiftsansvarig är den fysiska eller juridiska person (t.ex. aktiebolag, stiftelse, förening eller myndighet) som bestämmer för vilka ändamål uppgifter ska behandlas

[13] Ytterligare krav som ska regleras i ett avtal mellan personuppgiftsansvarig och biträde framgår av artikel 28 i dataskyddsförordningen, särskilt artikel 28.3 punkterna c) och e).

och hur behandlingen ska gå till.[14] Enligt patientdatalagen är en vårdgivare personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför, exempelvis vad gäller vårddokumentationen i den individinriktade vården.[15]

Personuppgiftsbiträde är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.[16] Personuppgiftsansvarige ska enbart anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas.[17] Personuppgiftsbiträden får som nämnts bara agera på instruktion av den personuppgiftsansvarige,[18] men dataskyddsförordningen ställer också krav på biträden att kontrollera att personuppgiftsbehandlingen uppfyller de krav som ställs i förordningen.[19]

Det är de faktiska omständigheterna i det enskilda fallet som avgör vem som är personuppgiftsansvarig respektive personuppgiftsbiträde.

Krav på öppenhet och information om vem som är personuppgiftsansvarig

De personer vars personuppgifter behandlas, här vårdsökande som ringer 1177, har enligt dataskyddsförordningen rätt att få information om hur deras personuppgifter behandlas.

Enligt dataskyddsförordningen ska personuppgifter behandlas på ett öppet sätt i förhållande till den registrerade.[20]

Förordningen innehåller krav på klar och tydlig information.[21] Det avser till exempel identitet och kontaktuppgifter för den personuppgiftsansvarige, ändamålen för och den rättsliga grunden med behandlingen samt kontaktuppgifter för dataskyddsombudet i förekommande fall.[22]

Informationen ska lämnas av den personuppgiftsansvarige när uppgifterna samlas in eller vid en senare tidpunkt om uppgifterna samlas in från någon annan källa.[23] Patientdatalagen innehåller ytterligare krav på information som ska lämnas av vårdgivaren till patienterna, exempelvis om de sekretess- och säkerhetsbestämmelser som gäller.[24]

På webbplatsen 1177.se informeras vårdsökande att det är vårdgivaren som ansvarar för att behandlingen av ens personuppgifter sker på ett lagligt och korrekt sätt.

Personuppgiftsansvaret innebär bland annat ett ansvar för att se till att man har ett rättsligt stöd för att behandla personuppgifterna och för att vidta erforderliga

[14] Dataskyddsförordningen artikel 4.7.
[15] 2 kap. 6 § och 2 kap. 4 § första stycket 1 och 2 patientdatalagen (2008:355).
[16] Dataskyddsförordningen artikel 4.8.
[17] Dataskyddsförordningen artikel 28.1.
[18] Dataskyddsförordningen artikel 28.3 a.
[19] Dataskyddsförordningen artikel 28.3 c.
[20] Dataskyddsförordningen artikel 5.1 a.
[21] Dataskyddsförordningen artikel 12.
[22] Dataskyddsförordningen artikel 13.
[23] Dataskyddsförordningen artikel 13.1 resp. 14.3.
[24] 8 kap. 6 § patientdatalagen.

säkerhetsåtgärder. Ansvaret innefattar också att behandla personuppgifter på ett öppet sätt i förhållande till de registrerade,[25] bl.a. genom att tillhandahålla tydlig information om vem som är personuppgiftsansvarig.[26]

På 1177.se ges informationen att om regionen är vårdgivare är det ”en eller flera styrelser eller nämnder i regionen som är ytterst ansvariga” och ”inom den privata vården är det företaget eller den verksamhet som bedriver vården som är ansvariga”.

Inkommande samtal till 1177 kopplas via en växel till en vårdgivare som besvarar samtalet från den vårdsökande. Det kan vara regionen som bedriver den hälso- och sjukvården i egen regi eller en vårdgivare som regionen anlitar. Under granskningen saknades information till personer som ringde 1177 från regionerna Stockholm, Värmland och Sörmland bland annat om vem som var vårdgivare enligt patientdatalagen och därmed personuppgiftsansvarig.

Tillsynsobjektens roller och ansvar och förhållandet dem emellan

Översiktlig beskrivning av informationsflödet

Samtal till 1177 styrs initialt till Inera, som tillhandahåller regionerna växel för att koppla samtal vidare. Hos Inera kontrolleras s.k. kommun-id, d.v.s. vilken kommun samtal kommer ifrån för att veta till vilken vårdgivare samtalet ska slussas. Regionerna Stockholm, Sörmland och Värmland[27] hade vid tiden för incidenten anlitat MedHelp som vårdgivare, varför Inera kopplade samtal från dessa kommuner till MedHelp.

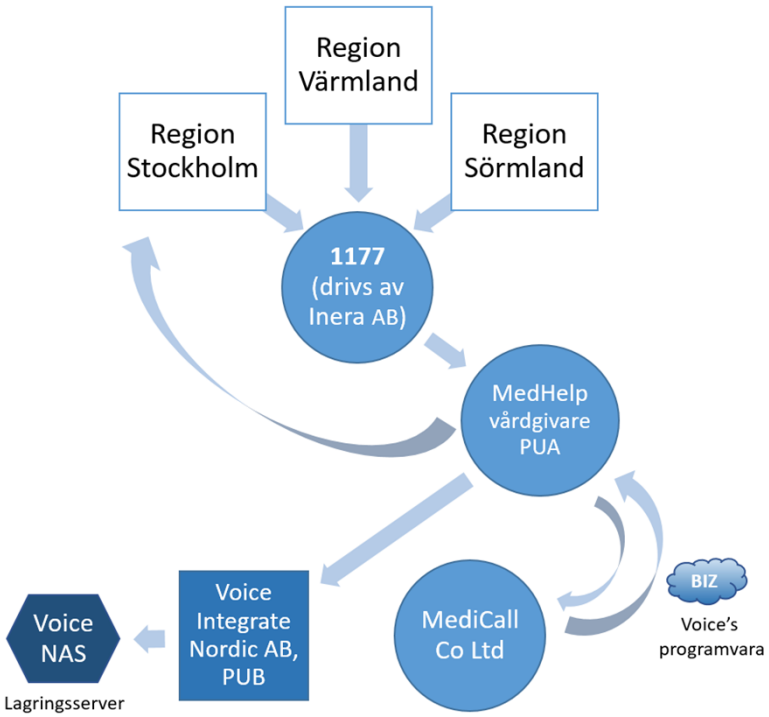
MedHelp hade i sin tur anlitat MediCall som personuppgiftsbiträde och underleverantör för sjukvårdsrådgivning via 1177 på telefon. MediCall är ett thailändskt bolag med verksamhet i Thailand, vars anställda sjuksköterskor besvarade samtal från vårdsökande under jourtid.

Voice hade utvecklat programvaran Biz för ljudinspelning och koppling av samtal från MedHelp till MediCall. Hos Voice fanns även servern Voice NAS.

Samtal som MediCall besvarade kom att överföras till Voice NAS för lagring. Från servern Voice NAS har samtalen sedan på grund av en säkerhetsbrist i samband med en felkonfigurering blivit exponerade mot internet. MedHelp förde efter att bristen upptäckts över vårddokumentationen till egna servrar och Voice raderade samtalen på MedHelps instruktion den 7 mars 2019.

[25] Dataskyddsförordningen artikel 5.1 a.
[26] Dataskyddsförordningen artikel 13.1 a.
[27] Regionerna Sörmland och Värmland övergick till att bedriva sjukvårdsrådgivningen via 1177 i egen regi under slutet av 2019.

Fig. 1, samtals- och informationsflöde mellan aktörerna.



Regionernas roller och ansvar

Regionerna Sörmland, Värmland och Stockholm är huvudmän med ansvar för hälso- och sjukvård[28] i sina respektive regioner. Huvudmän kan avtala med vårdgivare, som kan vara t.ex. myndigheter, kommuner eller företag, om att utföra den hälso- och sjukvård som huvudmännen ansvarar för.[29] De aktuella regionerna har ingått personuppgiftsbiträdesavtal med Inera för att låta vidarekoppla inkommande samtal till 1177 för att besvaras av MedHelp, som anlitats som vårdgivare.

De aktuella regionerna är personuppgiftsansvariga för behandlingen som sker när de samlar in uppgifter om telefonnummer och kommun-ID när enskilda ringer 1177 så att samtalen kan besvaras av MedHelp. Regionerna ansvarar därmed för att informera om den personuppgiftsbehandlingen.

Regionerna Sörmland och Värmland
Under granskningen har regionerna Sörmland och Värmland[30] upphört med att anlita MedHelp som vårdgivare för att besvara samtal till 1177.Integritetsskyddsmyndigheten (IMY)inte hade informerat vårdsökande om sin behandling av telefonnummer och uppgift om vilken kommun personen ringde ifrån.

IMY fann att bristen på information stred mot principen om öppenhet i dataskyddsförordningens artikel 5.1 a och mot artikel 13 om den information som ska tillhandahållas om personuppgifter samlas in från den registrerade.

---

[28] 2 kap. 2 § hälso- och sjukvårdslagen.
[29] 15 kap. 1 § hälso- och sjukvårdslagen.
[30] Regionstyrelsen i respektive region är personuppgiftsansvarig.

IMY beslutade mot den bakgrunden, att regionerna skulle betala en administrativ sanktionsavgift på 250 000 kronor vardera.

Region Stockholm
Utöver behandling av uppgifter om inringande personers telefonnummer och kommun-ID, för att kunna dirigera samtal till rätt vårdgivare, samlade Region Stockholm[31] även in personuppgifter från MedHelp. Insamlingen avsåg samtalsinformation från samtal till 1177 i regionen och omfattade bl.a. personnummer, kontaktorsak, koder för symtom, hänvisning (till t.ex. egenvård, närakut eller vårdcentral), verksamhets-id för vårdenheten där patienten eventuellt fått en bokad tid, löpnummer på journalanteckning (om sådan upprättats) och tidpunkt för samtal. Insamlingen av samtalsinformationen från MedHelp avsåg en omfattande mängd känsliga personuppgifter rörande ett stort antal registrerade.

Region Stockholm pseudonymiserar uppgifterna och använder informationen för att utveckla sjukvårdsrådgivningens funktion.

IMY konstaterade att Hälso- och sjukvårdsnämnden vid behandling av personuppgifter för att dirigera samtal till 1177 till vårdgivaren MedHelp inte hade informerat vårdsökande om sin behandling av telefonnummer och kommun-id. Hälso- och sjukvårdsnämnden informerade inte heller om insamlingen från MedHelp av personuppgifter om vårdsökande som ringt 1177.

IMY fann att bristen på information stred mot principen om öppenhet i artikel 5.1 a, samt mot artiklarna 13 och 14 i dataskyddsförordningen om den information som ska ges till vårdsökande.

IMY beslutade mot den bakgrunden att Hälso- och sjukvårdsnämnden skulle betala en administrativ sanktionsavgift på 500 000 kronor.

IMY förelade också enligt artikel 58.2 d i dataskyddsförordningen Hälso- och sjukvårdsnämnden att, snarast och senast två månader efter det att beslutet vunnit laga kraft, i enlighet med artiklarna 13 och 14 i dataskyddsförordningen informera vårdsökande som ringer 1177 om insamling av telefonnummer och kommun-id för ändamålet att tillse att samtal till 1177 tas om hand av vårdgivaren MedHelp AB samt om insamling av samtalsinformation från MedHelp AB för uppföljnings- och kvalitetsändamål.

Ineras roll och ansvar

Inera förvaltar och utvecklar de gemensamma system för 1177 och den därmed sammanhängande sjukvårdsrådgivning på telefon som regionerna behövde i sin verksamhet.[32] Inera bistod, som personuppgiftsbiträde, regionerna med hantering av inkommande samtal genom att koppla dem vidare till MedHelp. Inera spelade inte in dessa samtal. IMY avslutade tillsynen mot Inera utan åtgärd.

MedHelps roll och ansvar

Regionerna Stockholm, Sörmland och Värmland anlitade MedHelp som vårdgivare för att besvara vårdsökandens samtal till 1177. Samtal kopplades av Inera till MedHelp

[31] Hälso- och sjukvårdsnämnden är personuppgiftsansvarig i region Stockholm.
[32] www.inera.se/tjanster/1177-vardguiden-pa-telefon.

som tog över samtalet. MedHelp genomförde ungefär tre miljoner rådgivningssamtal per år via 1177.

Som vårdgivare och personuppgiftsansvarig behandlade MedHelp personuppgifter när enskilda ringde 1177. Personuppgiftsbehandlingen skedde genom inspelning av telefonsamtal och vårddokumentation i ett journalsystem.

MedHelp anlitade MediCall som personuppgiftsbiträde och underleverantör för sjukvårdsrådgivning via telefon när enskilda ringde 1177 under jourtid. Av de tre miljoner samtal per år som MedHelp mottog hanterades ungefär 20 procent hos MediCall.

MedHelp anlitade MediCall för att förbättra bemanningen vid jourtid. Då verksamheten bedrevs i Thailand kunde man dra nytta av tidsskillnaden för att erbjuda en högre tillgänglighet för sjukvårdsrådgivningen på 1177. MediCalls sjuksköterskor förde anteckningar i MedHelps journalsystem när samtal besvarades.

MedHelp har som personuppgiftsansvarig skyldighet att efterleva dataskyddsförordningen och nationell rätt för behandling av personuppgifter inom hälso- och sjukvården.[33] Ansvaret omfattar att fullgöra skyldigheterna i dataskyddsförordningen, inklusive skyldighet att behandla personuppgifter på ett öppet sätt i förhållande till de registrerade,[34] bl.a. genom att tillhandahålla tydlig information om behandlingen och om att MedHelp är personuppgiftsansvarig.[35]

IMY konstaterade att MedHelp i egenskap av vårdgivare och personuppgiftsansvarig hade behandlat personuppgifter i strid med dataskyddsförordningen, patientdatalagen och Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40) i följande avseenden:

– personuppgifter i ljudfiler med inspelade telefonsamtal till 1177 hade exponerats mot internet utan skydd i lagringsservern Voice NAS. MedHelp hade därvid i egenskap av vårdgivare och personuppgiftsansvarig underlåtit att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som var lämplig för att förhindra obehörigt röjande av personuppgifterna eller obehörig åtkomst till personuppgifterna.

– MedHelp hade utan lagligt stöd i svensk hälso- och sjukvårdslagstiftning och i dataskyddsförordningen låtit det thailändska bolaget MediCall, som inte omfattades av hälso- och sjukvårdslagen och bestämmelser om tystnadsplikt, utföra vård och behandla personuppgifter om vårdsökande som ringde 1177. Som stöd för den personuppgiftsbehandlingen upprättade MedHelp ett personuppgiftsbiträdesavtal med MediCall, men ett sådant avtal kan inte ersätta bristen på lagligt stöd.

– MedHelp hade inte, utöver ett talsvarsmeddelande om att samtalet spelades in i patientsäkerhets- och kvalitetssyfte, informerat vårdsökande som ringde 1177 om sin personuppgiftsbehandling.

– MedHelp hade inte säkerhetskopierat samtal till 1177 som MedHelp besvarade och spelade in i sin IT-miljö.

[33] Dataskyddsförordningen artikel 5.1 f.
[34] Dataskyddsförordningen artikel 5.1 a.
[35] Dataskyddsförordningen artikel 12.1.

IMY beslutade att MedHelp skulle betala en administrativ sanktionsavgift på 12 miljoner kronor, varav åtta miljoner kronor avsåg exponerade ljudfiler med inspelade telefonsamtal till 1177 mot internet utan skydd, tre miljoner kronor avsåg att MedHelp utfört personuppgiftsbehandling genom att anlita MediCall, femhundra tusen kronor avsåg att MedHelp inte lämnat nödvändig information till vårdsökande som ringde 1177 och femhundra tusen kronor avsåg att MedHelp inte hade säkerhetskopierat ljudfiler i sin IT-miljö.

Beslutet omfattade också två förelägganden. Ett avsåg information till vårdsökande vars samtal till 1177 besvaras av MedHelp.

Det andra föreläggandet avsåg att MedHelp ska genomföra säkerhetskopiering och förvara säkerhetskopiorna på ett säkert sätt väl skilda från originaluppgifterna,[36] samt att besluta om hur länge säkerhetskopiorna skulle sparas och hur ofta återläsningstester av kopiorna ska göras.[37]

Voice's roll och ansvar

Voice hade utvecklat programvaran Biz för ljudinspelning och koppling av samtal från MedHelp till MediCall. Hos Voice fanns även servern Voice NAS.

Voice är ett utvecklingsbolag som tar fram programvara. Voice och MedHelp hade enligt ett ingånget leveransavtal 2012 ett samarbete kring teknik, säkerhet och förbättringar inom tjänster och produktion. Företagen ingick ett personuppgiftsbiträdesavtal i maj 2018. Av avtalen framgår att uppdraget till Voice omfattade bl.a. sjukvårdsrådgivning och inspelning av samtal. Voice levererade samtal till MediCall via sina växlar genom programvaran Biz, och tillhandahöll även andra funktioner, program och support.

Inspelade ljudfiler med samtal till 1177 fanns i lagringsservern Voice NAS när incidenten inträffade.

IMY konstaterade att personuppgifter i ljudfiler med inspelade telefonsamtal till 1177 hade exponerats mot internet utan skydd i lagringsservern Voice NAS. Voice hade därvid i egenskap av personuppgiftsbiträde till MedHelp underlåtit att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som var lämplig för att förhindra obehörigt röjande av personuppgifterna eller obehörig åtkomst till personuppgifterna.

IMY beslutade att Voice skulle betala en administrativ sanktionsavgift på 650 000 kronor.

[36] Enligt 3 kap. 12 § HSLF-FS 2016:40.
[37] Enligt 3 kap. 13 § HSLF-FS 2016:40.