

MedHelp AB
Marieviksgatan 19
117 43 Stockholm

Diarienummer:
DI-2019-3375

Ert diarienummer:

Datum:
2021-06-07

Beslut efter tillsyn enligt dataskyddsförordningen mot MedHelp AB

Innehåll

Integritetsskyddsmyndighetens beslut.....	2
Bakgrund.....	3
Motivering av beslutet.....	3
Rättslig bakgrund.....	3
Nationella regler om hälso- och sjukvård.....	3
Personuppgiftsansvar och personuppgiftsbiträde.....	4
Grundläggande principer och rättslig grund.....	4
Registrerades rätt till information.....	5
Säkerhet i samband med behandlingen.....	5
MedHelps personuppgiftsansvar.....	6
Ansvaret för behandling av personuppgifter om vårdsökande som MediCall utfört.....	6
MedHelps uppgifter i tillsynsärendet.....	6
MediCalls uppgifter i incidentanmälan.....	7
IMY:s bedömning.....	7
Ansvaret för personuppgiftsincidenten i lagringsservern Voice NAS.....	10
Uppgifter från MedHelp, Medicall och Voice i incidentanmälningarna... ..	10
Uppgifter från Voice i tillsynsärendet DI-2019-2488.....	11
MedHelps uppgifter i tillsynsärendet.....	11
IMY:s bedömning.....	12
Skyldigheten att lämna information till vårdsökande.....	15
IMY:s bedömning.....	15
Ansvaret för säkerhetskopiering.....	17
IMY:s bedömning.....	17
Val av ingripande.....	18

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

Möjliga ingripandeåtgärder.....	18
Sanktionsavgift ska påföras.....	18
Fastställande av sanktionsavgiftens storlek.....	19
Generella bestämmelser.....	19
Sanktionsavgift för respektive överträdelse.....	20
Förelägganden.....	22
Hur man överklagar.....	23

Integritetsskyddsmyndighetens beslut

I egenskap av personuppgiftsansvarig vårdgivare enligt 2 kap. 6 § patientdatalagen (2008:355), PDL, har MedHelp AB (MedHelp) behandlat personuppgifter om vårdsökande i strid med dataskyddsförordningen¹ på följande sätt.

- a) Medhelp har under tiden den 25 maj 2018 till den 31 augusti 2019 genom att lämna ut personuppgifter till det thailändska bolaget MediCall och låta MediCall samla in personuppgifter behandlat personuppgifter i strid med artiklarna 5.1 a, 6 och 9.1 i dataskyddsförordningen.
- b) Medhelp har från okänt datum fram till den 18 februari 2019 i lagringsservern Voice NAS exponerat personuppgifter i ljudfiler med inspelade telefonsamtal till 1177² mot internet utan skydd mot obehörigt röjande av eller obehörig åtkomst till personuppgifterna. MedHelp har därigenom i strid med artiklarna 5.1 f och 32.1 i dataskyddsförordningen underlåtit att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå för uppgifterna.
- c) Medhelp har vid tiden för inspektionen den 20 mars 2019, utöver ett talsvarsmeddelande att samtalet spelas in i patientsäkerhets- och kvalitetssyfte, inte informerat vårdsökande om bolagets personuppgiftsbehandling i samband med insamlingen av personuppgifter vid telefonsamtal till 1177. MedHelp har därigenom behandlat personuppgifter i strid med artiklarna 5.1 a och 13 i dataskyddsförordningen.
- d) Medhelp har vid tiden för inspektionen den 20 mars 2019 inte säkerhetskopierat ljudfiler med inspelade samtal till 1177 som besvarats av MedHelps sjuksköterskor inom MedHelps telefonplattform. MedHelp har därigenom behandlat personuppgifter i strid med artiklarna 5.1 f och 32.1 i dataskyddsförordningen.

Integritetsskyddsmyndigheten (IMY) beslutar med stöd av artiklarna 58.2 och 83 i dataskyddsförordningen att MedHelp ska betala en administrativ sanktionsavgift på 12 000 000 (tolv miljoner) kronor för överträdelserna enligt följande. 3 000 000 (tre

¹ 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).

² På webbplatsen 1177.se anges "Ring telefonnummer 1177 för sjukvårdsrådgivning dygnet runt."

miljoner) kronor avser punkten a), 8 000 000 (åtta miljoner) kronor avser punkten b), 500 000 (femhundra tusen) kronor avser punkten c) och 500 000 (femhundra tusen) kronor avser punkten d).

IMY förelägger enligt artikel 58.2 d i dataskyddsförordningen MedHelp att snarast och senast två månader efter det att beslutet vunnit laga kraft vidta följande åtgärder.

1) Informera vårdsökande som ringer 1177 om MedHelps behandling av personuppgifter enligt artikel 13 i dataskyddsförordningen och 8 kap. 6 § PDL.

2) Beträffande ljudfiler med inspelade samtal till 1177, som besvaras av MedHelps sjuksköterskor inom MedHelps telefoniplattform, genomföra säkerhetskopiering med en fastställd periodicitet och förvara säkerhetskopior på ett säkert sätt väl skilda från originaluppgifterna enligt 3 kap. 12 § HSLF-FS 2016:40 samt besluta om hur länge säkerhetskopior ska sparas och hur ofta återläsningstester av kopiorna ska göras enligt 3 kap. 13 § HSLF-FS 2016:40.

Bakgrund

Computer Sweden publicerade den 18 februari 2019 en artikel med rubriken "2,7 miljoner inspelade samtal till 1177 Vårdguiden helt oskyddade på internet". I artikeln uppges bland annat att "På en öppen webbserver, helt utan lösenordsskydd eller annan säkerhet, har vi hittat 2,7 miljoner inspelade samtal till rådgivningsnumret 1177."

IMY inledde tillsyn mot MedHelp och genomförde en inspektion hos MedHelp den 20 mars 2019 för att kontrollera hur MedHelp behandlade personuppgifter inom ramen för 1177.

IMY inledde även tillsyn mot Voice Integrate Nordic AB (Voice) och Inera AB. Det framkom att tre regioner anlätade dels MedHelp som vårdgivare när vårdsökande ringer 1177 för sjukvårdsrådgivning och dels Inera AB för att koppla fram samtalen till MedHelp. IMY inledde därför tillsyn mot Hälso- och sjukvårdsnämnden Region Stockholm, Regionstyrelsen Region Sörmland och Regionstyrelsen Region Värmland.

Motivering av beslutet

Rättslig bakgrund

Nationella regler om hälso- och sjukvård

Hälso- och sjukvårdens uppdrag regleras i bland annat hälso- och sjukvårdslagen (2017:30), HSL.

Åtgärder för att medicinskt förebygga, utreda och behandla sjukdomar och skador definieras som hälso- och sjukvård, 2 kap. 1 § HSL. Med huvudman avses den region eller den kommun som enligt lagen ansvarar för att erbjuda hälso- och sjukvård till befolkningen i regionen eller kommunen. Inom en huvudmans geografiska område kan en eller flera vårdgivare bedriva verksamhet, 2 kap. 2 § HSL. Med vårdgivare avses statlig myndighet, region, kommun, annan juridisk person eller enskild näringsidkare som bedriver hälso- och sjukvårdsverksamhet, 2 kap. 3 § HSL. Regioner och kommuner får med bibehållet huvudmannaskap sluta avtal med någon annan om att utföra de uppgifter som landstinget eller kommunen ansvarar för, 15 kap. 1 § HSL. Den som har ett författningsreglerat ansvar för att vård ges betecknas huvudman.

Ansvarer innebär inte en skyldighet att själv bedriva verksamheten, utan driften kan ligga på någon annan som då betecknas vårdgivare (prop. 1981/82:97 s. 33 f.). Det offentliga ansvaret som huvudman innebär inte bestämmanderätt över vårdgivarens dagliga verksamhet och det fråntar inte heller vårdgivaren ansvaret som följer med rollen som vårdgivare (prop. 2016/17:43 s. 86).

Den som tillhör eller har tillhört hälso- och sjukvårdspersonalen inom den enskilda hälso- och sjukvården får enligt 6 kap. 12–15 §§ patientsäkerhetslagen (2010:659), (PSL) inte obehörigen röja vad han eller hon i sin verksamhet har fått veta om en enskilds hälsotillstånd eller andra personliga förhållanden. För det allmänna verksamhet gäller offentlighets- och sekretesslagen (2009:400) OSL.

Personuppgiftsansvar och personuppgiftsbiträde

Med personuppgiftsansvarig avses, enligt artikel 4.7 i dataskyddsförordningen, en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.

Enligt 2 kap. 6 § PDL är en vårdgivare personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför i samband med individinriktad vård i sin verksamhet, exempelvis vad gäller skyldigheten att föra patientjournal.

Enligt artikel 24 i dataskyddsförordningen ska den personuppgiftsansvarige med beaktande av behandlingens art, omfattning, sammanhang och ändamål, samt riskerna, genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa – och kunna visa – att behandlingen utförs i enlighet med dataskyddsförordningen.

Med personuppgiftsbiträde avses, enligt artikel 4.8 i dataskyddsförordningen, en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Personuppgiftsbiträdet får enligt artikel 29 i dataskyddsförordningen endast behandla personuppgifter på den personuppgiftsansvariges instruktion.

Grundläggande principer och rättslig grund

Personuppgifter ska enligt artikel 5.1 a i dataskyddsförordningen behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (principen om laglighet, korrekthet och öppenhet). Enligt artikel 5.1 f ska personuppgifter 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 (principen om integritet och konfidentialitet). Personuppgiftsansvariga ska enligt artikel 5.2 ansvara för och kunna visa att principerna i artikel 5.1 efterlevs (principen om ansvarsskyldighet).

För att en behandling av personuppgifter ska vara laglig krävs att den har stöd i någon av de rättsliga grunder som anges i artikel 6.1 i dataskyddsförordningen. Vid behandling för hälso- och sjukvårdsändamål är det främst artikel 6.1 c (rättslig förpliktelse) eller 6.1.e (allmänt intresse eller myndighetsutövning) som kan vara tillämpliga. Enligt artikel 6.3 ska den grund för behandlingen som anges i artikel 6.1 c och e fastställas i enlighet med unionsrätten eller en medlemsstats nationella rätt som

den personuppgiftsansvarige omfattas av. Det innebär att om en vårdgivares behandling av personuppgifter är nödvändig för att fullgöra en rättslig förpliktelse eller utföra en uppgift av allmänt intresse så krävs för att behandlingen ska vara laglig att den rättsliga förpliktelsen eller uppgiften av allmänt intresse regleras i nationell rätt (eller i unionsrätten).

För verksamhet enligt bland annat HSL finns kompletterande dataskyddsbestämmelser främst i PDL och i HSLF-FS 2016:40, som bland annat innehåller regler om informationssäkerhet och om fysiskt skydd av informationssystem.

Enligt 1 kap. 2 § PDL ska informationshantering inom hälso- och sjukvården vara organiserad så att den tillgodoser patientsäkerhet och god kvalitet samt främjar kostnadseffektivitet. Personuppgifter ska utformas och i övrigt behandlas så att patienters och övriga registrerades integritet respekteras. Dokumenterade personuppgifter ska hanteras och förvaras så att obehöriga inte får tillgång till dem.

Uppgifter om hälsa utgör så kallade känsliga personuppgifter. Det är förbjudet att behandla sådana personuppgifter enligt artikel 9.1 i dataskyddsförordningen, såvida behandlingen inte omfattas av något av undantagen i artikel 9.2.

Registrerades rätt till information

Personuppgiftsansvarigas skyldighet att självmant tillhandahålla registrerade information om behandlingen av personuppgifterna framgår av artiklarna 13 och 14 i dataskyddsförordningen. Det är förhållandevis omfattande upplysningar som ska lämnas till de registrerade. Utöver vad som framgår av artiklarna 13 och 14 ska den vårdgivare som är personuppgiftsansvarig enligt 2 kap. 6 § PDL lämna ytterligare information enligt 8 kap. 6 § PDL till den registrerade. Informationen enligt 8 kap. 6 § PDL ska omfatta bland annat vad som gäller i fråga om sökbegrepp, direktåtkomst och utlämnande av uppgifter på medium för automatiserad behandling.

Säkerhet i samband med behandlingen

Enligt artikel 32.1 i dataskyddsförordningen ska både den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå till skydd för de uppgifter som behandlas. Vid bedömningen av vilka tekniska och organisatoriska åtgärder som är lämpliga ska den personuppgiftsansvarige och personuppgiftsbiträdet beakta den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter. Enligt artikel 32.1 omfattar lämpliga skyddsåtgärder, 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, och d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Enligt artikel 32.2 i dataskyddsförordningen ska vid bedömningen av lämplig säkerhetsnivå särskild hänsyn tas till de risker som behandlingen medför, i synnerhet för 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.

Socialstyrelsen har i HSLF-FS 2016:40 med stöd av 3 § patientdataförordningen (2008:360) och efter samråd med IMY meddelat föreskrifter som behövs för verkställigheten av PDL i fråga om säkerhetsåtgärder vid helt eller delvis automatiserad behandling av personuppgifter. En personuppgiftsansvarig vårdgivare ska enligt 3 kap. 12 § HSLF-FS 2016:40 säkerställa att personuppgifter som behandlas i informationssystem säkerhetskopieras med en fastställd periodicitet och att säkerhetskopiorna förvaras på ett säkert sätt, väl åtskilda från originaluppgifterna. Föreskriften preciserar i 3 kap. 12 § således en säkerhetsåtgärd som ska vidtas av personuppgiftsansvariga. Vårdgivaren ska enligt 3 kap. 13 § besluta om hur länge säkerhetskopiorna ska sparas och hur ofta återläsningstester av kopiorna ska göras.

MedHelps personuppgiftsansvar

Av MedHelps anmälan av en personuppgiftsincident den 20 februari 2019 (IMY:s ärende PUI-2019-689) framgår att MedHelp uppger sig vara personuppgiftsansvarig såvitt avser behandling av känsliga personuppgifter i form av ljudfiler som har exponerats mot internet utan några skyddsmekanismer.

I detta tillsynsärende uppger MedHelp att bolaget är vårdgivare enligt definitionen i 1 kap. 3 § PDL och därmed personuppgiftsansvarig enligt 2 kap. 6 § samma lag för de personuppgifter som bolaget behandlar när enskilda ringer 1177. Bolaget uppger vidare att, som ett komplement till journalanteckningarna, sparas samtalen genom att spelas in och lagras. Dessa inspelningar är en del av vårddokumentationen. MedHelp anser sig vara personuppgiftsansvarig för de filer som lagrats på servern hos Voice för MediCalls räkning. Då samtalen inte kunde lagras hos Voice längre fördes de över till MedHelps servrar.

IMY delar MedHelps uppfattning att MedHelp är personuppgiftsansvarig vårdgivare enligt 2 kap. 6 PDL och att MedHelp för den individriktade vård som sker i samband med att enskilda ringer 1177 får behandla personuppgifter för ändamål som rör vårddokumentation, exempelvis genom inspelning av samtal till 1177.

Ansvar för behandling av personuppgifter om vårdsökande som MediCall utfört

MedHelps uppgifter i tillsynsärendet

Beträffande MediCalls roll vid sjukvårdsrådgivning via telefon har MedHelp bland annat uppgett följande.

MedHelp har anlitat MediCall som underleverantör för sjukvårdsrådgivning via telefon när enskilda ringer 1177. MediCall är ett thailändskt bolag med verksamhet i Thailand. MedHelp mottar cirka 3 miljoner samtal per år inom ramen för 1177. 20 procent av trafiken går till MediCall och resten till MedHelp. Alla sjuksköterskor har svensk sjuksköterskelegitimation och uppfyller kraven i avtalen med regionerna. Sjuksköterskorna som jobbar för MediCall är anställda av MediCall. Sjuksköterskor hos både MedHelp och MediCall för anteckningar i MedHelps journalsystem Princess och det sker inspelning av telefonsamtalen till 1177.

MedHelp är ansvarig vårdgivare. Vårdgivare och patient befinner sig i Sverige när vården ges. MediCall är journalföringspliktigt. För att spela in samtalen används intresseavvägning som rättslig grund.

MedHelp ingick den 15 oktober 2012 ett avtal med MediCall avseende sjukvårdsrådgivning och i samband med det slöts ett personuppgiftsbiträdesavtal. Parterna ingick den 1 oktober 2016 ett tilläggsavtal och ett nytt avtal benämnt "Avtal avseende sjukvårdsrådgivningstjänster på telefon". Ett tilläggsavtal till detta avtal upprättades och undertecknades den 1–2 mars 2019. I bilaga 4 till tilläggsavtalet finns även ett nytt personuppgiftsbiträdesavtal som ersätter det tidigare personuppgiftsbiträdesavtalet från 2012. MedHelp har uppgett att avtalet och personuppgiftsbiträdesavtalet upphör den 31 augusti 2019, varvid även MediCalls behandling av personuppgifter relaterade till 1177 upphör.

MediCalls uppgifter i incidentanmälan

Efter att IMY ställt frågor till MediCall har MediCall den 19 juni 2019 kompletterat sin anmälan av personuppgiftsincidenten och därvid uppgett bland annat följande.

MediCall är ett thailändskt bolag, som tillhandahåller rådgivning per telefon och andra kommunikationsvägar i enlighet med MedHelps standards och rutiner på uppdrag av MedHelp. Verksamheten bedrivs enbart i Thailand. Personuppgifterna kommer till tjänstgörande sjuksköterska via MedHelps journalsystem på en skärm. Sjuksköterskan svarar och ser information baserat på vad den inringande knappat in. Efter samtalet eller under samtalets gång förs en journal. När samtalet avslutats stängs journalen ner och kan ej öppnas av sjuksköterskan igen. Samtalet lagras i MedHelps system direkt. MediCall ser alltså journalen i MedHelps system, arbetar i systemet, och dokumenterar i MedHelps system, ingen information sparas av MediCall. It-systemet heter Collab.

När incidenten inträffade kom samtalen in via Biz, som hanterar inkommande och utgående samtal. Samtalen spelades in av Biz och lagrades av Voice på uppdrag av MedHelp. MediCall har i sitt avtal 2012-09-02 med MedHelp en klausul som föreskriver att behandling av personuppgifter ska ske enligt gällande lag. Nytt personuppgiftsbiträdesavtal inklusive avtal om sekretess tecknades den 1 mars 2019. MediCall har angett Voice som personuppgiftsbiträde men är lite osäkra i denna fråga då MediCall ser dem som leverantör direkt till MedHelp. Inget personuppgiftsbiträdesavtal mellan MediCall och Voice har tecknats.

Den 29 augusti 2019 har MediCall på eget initiativ gett in ett dokument till IMY som komplettering till sin anmälan av personuppgiftsincident. Överst i dokumentet, som är daterat den 30 oktober 2012, anges Hälso- och sjukvårdsförvaltningen, Stockholms läns landsting, diarienummer HSN 0805-0652 och ämnet "Angående begäran om godkännande av underleverantör". Under rubriken "Beskriv hur ni säkerställer att avtalet uppfylls med hjälp av underleverantören avseende punkterna" framgår bland annat att MedHelp gör detta för att förbättra bemanningen vid jourtid vilket kommer ge en högre tillgänglighet för sjukvårdsrådgivningen per telefon åt Vårdguiden (punkt 3). I punkt 5 anges att samtliga tjänster som MediCall utför kommer följa MedHelps kvalitetsledningssystem.

IMY:s bedömning

Svensk hälso- och sjukvård har en omfattande reglering. Utöver bestämmelserna i dataskyddsförordningen är HSL av central betydelse. Lagen innehåller bestämmelser om hur svensk hälso- och sjukvårdsverksamhet ska organiseras och bedrivas. Åtgärder för att medicinskt förebygga, utreda och behandla sjukdomar och skador definieras som hälso- och sjukvård, 2 kap. 1 § HSL. Med huvudman avses den region eller den kommun som enligt lagen ansvarar för att erbjuda hälso- och sjukvård till befolkningen i regionen eller kommunen. Inom en huvudmans geografiska område kan en eller flera vårdgivare bedriva verksamhet, 2 kap. 2 § HSL. Med vårdgivare avses

statlig myndighet, region, kommun, annan juridisk person eller enskild näringsidkare som bedriver hälso- och sjukvårdsverksamhet, 2 kap. 3 § HSL.

Regioner och kommuner får med bibehållet huvudmannaskap sluta avtal med någon annan om att utföra de uppgifter som landstinget eller kommunen ansvarar för, 15 kap. 1 § HSL. Den som har ett författningsreglerat ansvar för att vård ges betecknas huvudman. Ansvaret innebär inte en skyldighet att själv bedriva verksamheten, utan driften kan ligga på någon annan som då betecknas vårdgivare (prop. 1981/82:97 s. 33 f.). Det offentliga ansvaret som huvudman innebär inte bestämmanderätt över vårdgivarens dagliga verksamhet och det fräntar inte heller vårdgivaren ansvaret som följer med rollen som vårdgivare (prop. 2016/17:43 s. 86).

MedHelp är personuppgiftsansvarig vårdgivare för den behandling av personuppgifter som sker i samband med den sjukvårdsrådgivning som MedHelp har fått i uppdrag av regionerna att utföra. Det innebär att MedHelp enligt artikel 5.2 i dataskyddsförordningen ska kunna visa att personuppgifterna behandlas på ett sätt så att principerna i artikel 5.1 efterlevs.

För att en behandling av personuppgifter ska vara laglig krävs att den har stöd i någon av de rättsliga grunder som anges i artikel 6.1 i dataskyddsförordningen. Vid behandling för hälso- och sjukvårdsändamål är det främst artikel 6.1 c (rättslig förpliktelse) eller 6.1 e (allmänt intresse eller myndighetsutövning) som kan vara tillämpliga. Enligt artikel 6.3 ska den grund för behandlingen som anges i artikel 6.1 c och e fastställas i enlighet med unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av. Det innebär att om en vårdgivares behandling av personuppgifter är nödvändig för att fullgöra en rättslig förpliktelse eller utföra en uppgift av allmänt intresse så krävs för att behandlingen ska vara laglig att den rättsliga förpliktelsen eller uppgiften av allmänt intresse regleras i nationell rätt (eller i unionsrätten).

Inom hälso- och sjukvården kompletteras dataskyddsförordningen av PDL, som innehåller bestämmelser bland annat om vem som är personuppgiftsansvarig, om skyldigheten att föra patientjournal och om tillåtna ändamål för behandling av personuppgifter. Enligt 1 kap. 3 § PDL omfattar PDL:s tillämpningsområde verksamhet som avses i bland annat hälso- och sjukvårdslagen (2017:30), HSL. Fastställandet i 2 kap. 6 § PDL av att vårdgivaren är personuppgiftsansvarig är en nationell precisering av artikel 4.7 i dataskyddsförordningen.

En vårdgivare behöver behandla uppgifter om hälsa och ibland även andra särskilda kategorier av personuppgifter enligt artikel 9.1 i dataskyddsförordningen, s.k. känsliga personuppgifter. Det är som utgångspunkt förbjudet att behandla känsliga personuppgifter enligt samma artikel. De undantag som finns från förbudet framgår av artikel 9.2. För hälso- och sjukvård finns ett undantag i artikel 9.2.h som är tillämpligt under förutsättning att det finns en lagreglerad tystnadsplikt enligt artikel 9.3.

För svensk hälso- och sjukvård är det huvudsakligen regleringen i HSL och PDL samt av tystnadsplikten i OSL och i 6 kap. 12-15 §§ PSL som anger det rättsliga stödet för att en behandling av personuppgifter är laglig på det sätt som avses i artikel 6.1 e, 6.2 och 6.3 samt 9.2 h och 9.3 i dataskyddsförordningen (prop. 2017/18:105 s. 58 och 94 samt prop. 2017/18:171 s. 105).

Genom såväl MedHelps som MediCalls uppgifter har det framkommit att både MedHelp och MediCall har vidtagit åtgärder som faller in under begreppet hälso- och

sjukvård enligt definitionen i 2 kap. 1 § HSL såvitt avser 1177 genom sina åtgärder för att medicinskt förebygga, utreda och behandla sjukdomar och skador. Förhållandet är reglerat genom avtal och personuppgiftsbiträdesavtal. MediCall har för att kunna utföra vården behandlat personuppgifter. Det har skett genom att MediCall tagit del av personuppgifter gällande vårdsökande på en dataskärm via MedHelps journalsystem och genom att svara vid uppringning på 1177. MediCall har under samtalet samlat in personuppgifter genom att föra in vårddokumentation i MedHelps journalsystem vilket också inneburit en behandling av personuppgifter.

MediCall är emellertid ett thailändskt bolag som bedriver verksamheten i Thailand. Det innebär de svenska bestämmelserna på hälso- och sjukvårdens område inte är tillämpliga, även om sjuksköterskorna som arbetar hos MediCall har svensk legitimation. MediCall har således inte ålagts nationella uppgifter och ansvar genom bestämmelserna i HSL och är inte vårdgivare enligt svensk rätt. MediCall omfattas därför inte heller av tillämpningsområdet för PDL enligt 1 kap. 3 § PDL, där det anges att PDL tillämpas vid vårdgivares behandling av personuppgifter inom hälso- och sjukvården. Det innebär vidare att MediCall inte kan vara journalföringspliktigt enligt 3 kap. PDL, såsom MedHelp uppgett.

Tystnadsplikten för privata vårdgivare regleras i 6 kap. 12–15 §§ PSL. Det anges, som huvudregel, att den som tillhör eller tillhört hälso- och sjukvårdspersonal inom den enskilda hälso- och sjukvården inte får obehörigen röja vad han eller hon i sin verksamhet har fått vet om en enskilds hälsotillstånd eller andra personliga förhållanden. Av 1 kap. 2 § PSL framgår att med hälso- och sjukvård avses i PSL verksamhet som omfattas av HSL eller andra nationella regleringar på hälso- och sjukvårdsområdet som exempelvis tandvårdslagen, lagen om försäkringsmedicinska utredningar m.fl. Verksamheten i MediCall omfattas inte av de nationella bestämmelserna vare sig i HSL eller i någon av de andra angivna författningarna vilket innebär att inte heller 6 kap. PSL är tillämpligt. MediCall saknar därför en enligt svensk rätt reglerad tystnadsplikt.

Bestämmelserna i 6 kap. PDL om sammanhållen journalföring och i 25 kap. 11 § 3 OSL innebär att två eller flera svenska vårdgivare kan inleda ett frivilligt samarbete i vårdsyfte genom att följa bestämmelserna i 6 kap. PDL (jfr prop. 2007/08:126 s. 132 f om att den enskilda hälso- och sjukvården kan söka ledning för bedömningar av tystnadsplikten i sekretessbestämmelser). Om MediCall varit en svensk vårdgivare – dvs. omfattats av HSL, PSL och PDL – hade MedHelp och MediCall kunnat inleda ett frivilligt samarbete i vårdsyfte genom att följa bestämmelserna i 6 kap. PDL om sammanhållen journalföring.

MedHelp är vårdgivare och det rättsliga stödet för behandlingen av här aktuella personuppgifter är rättslig förpliktelse eller allmänt intresse enligt artikel 6.1 c eller e i dataskyddsförordningen, som fastställts i svensk rätt i författningar såsom PDL och HSL i enlighet med artikel 6.3 i dataskyddsförordningen. Rättsligt stöd för att få behandla känsliga personuppgifter trots förbudet i artikel 9.1 finns i artikel 9.2 h och 9.3. Intresseavvägning enligt artikel 6.1 f i dataskyddsförordningen är i detta sammanhang inte en tillämplig rättslig grund.

MedHelp har genom att anlita MediCall som underleverantör för sjukvårdsrådgivning via telefon när enskilda ringer 1177 bedrivit hälso- och sjukvård och har därvid låtit MediCall behandla personuppgifter utan rättsligt stöd i svensk rätt och utan att det föreligger en lagreglerad tystnadsplikt på det sätt som krävs enligt artikel 9.3 i dataskyddsförordningen.

MedHelp ingick den 15 oktober 2012 ett avtal med MediCall avseende "Sjukvårdsrådgivning" och i samband med det slöts ett personuppgiftsbiträdesavtal. Parterna ingick den 1 oktober 2016 ett tilläggsavtal och ett nytt avtal benämnt "Avtal avseende sjukvårdsrådgivningstjänster på telefon". Ett tilläggsavtal till detta avtal upprättades och undertecknades den 1–2 mars 2019. I bilaga 4 till tilläggsavtalet finns även ett nytt personuppgiftsbiträdesavtal som ersätter det tidigare personuppgiftsbiträdesavtalet från 2012.

Det förhållandet att de svenska reglerna gällande hälso- och sjukvård inte gäller för ett thailändskt bolag kan inte ersättas med ett personuppgiftsbiträdesavtal eller någon annan avtalskonstruktion. Med personuppgiftsbiträde avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning, artikel 4.8 i dataskyddsförordningen. MediCall bedriver vård och kan inte utgöra ett personuppgiftsbiträde i det sammanhanget, då en vårdgivare måste ha ett självständigt stöd för att behandla personuppgifter, vilket MediCall saknar.

IMY konstaterar att MedHelp, som personuppgiftsansvarig vårdgivare enligt 2 kap. 6 § PDL, i vart fall från den 25 maj 2018 till den 31 augusti 2019 i samband med att vårdsökande ringer 1177 för sjukvårdsrådgivning lämnat ut personuppgifter dels på dataskärm, dels via telefon till MediCall samt låtit MediCall samla in personuppgifter för MedHelps vårddokumentation trots att MediCall inte omfattas av HSL och därmed inte heller omfattas av bestämmelserna i PSL och PDL. Dessa behandlingar har saknat rättsligt stöd i svensk rätt på det sätt som krävs enligt artikel 6.3 och utförts utan att det föreligger en lagreglerad tystnadsplikt på det sätt som krävs enligt artikel 9.3 i dataskyddsförordningen. Behandlingarna har således saknat laglig grund enligt artikel 6 och utförts i strid mot förbudet att behandla känsliga personuppgifter i artikel 9.1 i dataskyddsförordningen. Därigenom har behandlingen även skett i strid med principen om laglighet i artikel 5.1 a i dataskyddsförordningen.

Ansvaret för personuppgiftsincidenten i lagringsservern Voice NAS

Uppgifter från MedHelp, Medical och Voice i incidentanmälningarna

I MedHelps anmälan av personuppgiftsincident beskrivs incidenten som att känsliga personuppgifter hade exponerats mot internet utan några skyddsmekanismer och att ett okänt antal ljudfiler varit tillgängliga. Incidenten rör patienter och anställda hos den personuppgiftsansvariges underleverantör. Personuppgifter som omfattats av incidenten anges vara hälsa, sexualliv, personnummer, födelsedatum, identifierande information, till exempel för- och efternamn samt kontaktinformation. Vidare framgår att MedHelp fick kännedom om personuppgiftsincidenten av Inera AB:s vice vd.

IMY mottog den 21 februari 2019 MediCalls anmälan av en personuppgiftsincident (IMY:s ärende PUI-2019-698). Incidenten beskrivs som "Intrång i underleverantörs (Voice Integrate Nordic ab) server." Incidenten rör patienter. Personuppgifter som omfattats av incidenten anges vara hälsa, personnummer och identifierande information, till exempel för- och efternamn. Efter att IMY ställt frågor till MediCall uppgav MediCall den 19 juni 2019 bland annat att samtalen lagrades hos Voice på uppdrag av MedHelp.

IMY mottog den 21 februari 2019 Voice:s anmälan av personuppgiftsincident (IMY:s ärende PUI-2019-705). Incidenten beskrivs som att ett säkerhetshål i en lagringsserver upptäcktes av Computer Sweden som publicerade denna information i en artikel.

Incidenten rör patienter och företagsanvändare i mindre omfattning. Personuppgifter som omfattats av incidenten anges vara hälsa, personnummer, identifierande information till exempel för- och efternamn samt kontaktinformation.

Uppgifter från Voice i tillsynsärendet DI-2019-2488

Voice har bland annat uppgett följande.

Voice stängde ned lagringsservern den 18 februari 2019 och ändrade så att servern inte längre var nåbar via internet genom att ip-tables (ett brandväggsverktyg för att tillåta eller blockera åtkomstmöjligheter i nätverk) infördes direkt i servern. Efter att incidenten uppmärksammats ville MedHelp att it-forensiker skulle undersöka lagringsservern Voice NAS. MedHelp fick därför tillstånd att komma in på Voice NAS den 20 februari 2019. MedHelp ska även ha börjat flytta över innehållet i Voice NAS till MedHelps egna servrar. Om flytten av uppgifterna skedde genom enbart kopiering av filerna eller genom att filerna togs bort i samband med kopieringen var okänt för Voice. Voice har uppgett på IMY:s fråga den 14 mars 2019, om det fanns några samtalsfiler kvar på Voice NAS, att samtalen hade raderats på begäran av MedHelp den 7 mars 2019.

Voice och MedHelp har ingått "Leveransavtal – tjänster" undertecknat den 1 september 2012. Enligt avtalet har Voice och MedHelp sedan många år haft ett tätt samarbete inom teknik, säkerhet och möjliga förbättringar inom både teknik, tjänster samt produktion. Avtalet beskriver tjänster som "Recording (inom system) CC-50, "Inspelning av samtal", "Sökfunktioner för återsökning" och "Filtrering eller borttagning av inspelningar enligt kunds önskemål". Leveransavtalet gäller fr.o.m. 2012-09-01 t.o.m. 2019-06-30.

Per den 18 februari 2019 fanns 2,7 miljoner filer på lagringsservern Voice NAS, att dessa filer inte motsvarar 2,7 miljoner samtal, men att ett samtal motsvarar i genomsnitt cirka tre till fyra filer och att ett samtal kan utgöra upp till tio filer.

Det uppstår ett samtalsflöde när en person ringer till 1177. De inspelade samtalen är samtal från personer som ringt 1177 sjukvårdsupplysningen och sedan kopplas vidare till MedHelp och MediCall.

Voice uppdrag enligt avtal med MedHelp och MediCall har varit att leverera samtal via sina växlar samt ge support för funktioner och programvaror som omfattats av avtalet. Voice har tagit fram programvaran Biz. Det är riktigt att datafiler med inspelade samtal kommit att överföras från MedHelp till Voice NAS, en nätverksansluten lagringsenhet. Det har föranletts av att Medhelps egen server hade kraschat. Medhelps serverproblem började redan 2013 för att därefter eskalera och leda till en akut situation hösten 2015. Voice ledning deltog inte i detta beslut eller verkställde det, utan fick kännedom om att filerna fanns där den 18 februari 2019 när incidenten uppmärksammades i media.

Inga inspelningar skulle ha lagrats hos Voice. En månad innan dataskyddsförordningen skulle träda i kraft skickade MedHelp plötsligt över ett personuppgiftsbiträdesavtal. Något sådant hade inte tidigare funnits mellan parterna. Avtalet presenterades som ett standardavtal som alla avtalsparter behövde ingå inför att dataskyddsförordningen trädde i kraft.

MedHelps uppgifter i tillsynsärendet

MedHelp har uppgett bland annat följande i detta tillsynsärende.

MedHelp kände till att MediCall lagrade samtal hos Voice, men MedHelp kände inte till att servern gjorts nåbar utan skyddsmekanismer från internet. Medicalls sjuksköterskor kopplades till Medhelps nät från den 23 februari 2019, istället för till telefonlösningen Biz hos Voice. Detta innebär att samtalen som ringdes in omdirigerades till Medhelps servrar och infrastruktur, bland annat till Collab som är en telefonlösning som Medhelp själva driftar.

MedHelp mottar cirka 3 miljoner samtal per år inom ramen för 1177. Åttio procent av dessa hanteras av MedHelp och tjugo procent hanteras av Medicall, som tidigare använde it-lösningen Biz där det ingår ljudfilslagring. Voice hade byggt en webbapplikation som gör att man ska kunna lyssna på ljudfilerna. MedHelp har använt applikationen för samtalsuppföljning. För att kunna ta del av inspelningar har MedHelps personal varit tvungen att vara inloggad i MedHelps interna miljö och utöver det även autentisera sig i webbapplikationen. Av för MedHelp okänd anledning kom det lagrade innehållet sedan ut på nätet. Då samtalen inte kunde lagras hos Voice längre fördes de över till MedHelps servrar. MedHelps lagringsenheter har aldrig kraschat. MedHelp hade inte några serverproblem som ledde till en akut situation hösten 2015. Det har aldrig skett någon överföring av datafiler med inspelade patientsamtal från MedHelp till Voice. MedHelp har vid all tid lagrat inspelningar av patientsamtal uteslutande i egen regi på egna lagringsenheter. Voice har aldrig lagrat inspelningar på uppdrag av MedHelp. Däremot har Voice lagrat inspelningar av patientsamtal på uppdrag av MedHelps underleverantör MediCall.

Ett avtal benämnt "Personuppgiftsbiträdesavtal" undertecknades av MedHelp den 7 maj 2018 och av Voice den 10 maj 2018. Voice benämns som leverantören i avtalet, där bland annat framgår följande. MedHelp har ingått avtal med kunder och partners t.ex. vad avser ett avtal om att MedHelp ska tillhandahålla sjukvårdsrådgivning till kunder och partners. Avtalet reglerar MedHelp-koncernens överlämnande av personuppgifter till leverantören i anledning av tjänsteavtal och övriga avtal träffade mellan MedHelp och leverantören. Av punkt 11 framgår att MedHelp har rätt att efter skäligt varsel och på lämpligt sätt bereda sig och/eller dennes representant möjlighet att inspektera att leverantörens behandling av personuppgifter sker i överensstämmelse med tjänsteavtal och att leverantören har vidtagit lämpliga säkerhetsåtgärder för att skydda de personuppgifter som behandlas på uppdrag av MedHelp-koncernen. Vidare framgår bland annat att part ska löpande under avtalsperioden genomföra kontroll av att informationssäkerhetsarbetet är i enlighet med vid var tid gällande lagar och förordningar vilket bland annat innebär att part ska genomföra interna granskningar, skyddsåtgärder samt riskanalyser.

IMY:s bedömning

Ljudfilerna i lagringsservern Voice NAS hos Voice innehöll inspelade samtal till 1177 som sjuksköterskor hos MediCall besvarat. Såsom konstateras ovan är MedHelp i egenskap av vårdgivare personuppgiftsansvarig för dessa personuppgifter. Personuppgiftsansvaret omfattar ett ansvar för att personuppgifterna behandlas i enlighet med gällande dataskyddsregler. Det framgår bland annat av de grundläggande principerna i artikel 5 och av artikel 24. Det omfattar enligt artikel 5.2 också att man ska kunna visa att man gör det.

Att MedHelp genom avtal låtit MediCall och Voice behandla personuppgifterna påverkar inte omfattningen av MedHelps ansvar. Det är den personuppgiftsansvarige som har det yttersta ansvaret för en korrekt och laglig behandling av personuppgifterna. MedHelp har därvid också ansvaret för säkerheten i samband med behandlingen.

Såsom konstaterats tidigare är det frågan om personuppgifter som dokumenterats i samband med sjukvårdsrådgivning när vårdsökande ringt 1177 i regionerna Stockholm, Sörmland och Värmland. Det är frågan om en verksamhet som MedHelp är vårdgivare och därmed personuppgiftsansvarig för. MedHelp måste därför i egenskap av personuppgiftsansvarig vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandlingen 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, artikel 32.1 och 2 i dataskyddsförordningen. Att säkerställa en lämplig säkerhet innebär att man måste anpassa säkerhetsnivån till riskerna för den aktuella behandlingen.

Medicalls behandling avsåg 20 procent av de cirka 3 miljoner telefonsamtal som MedHelp tog emot årligen via 1177, totalt ca 600 000 samtal per år. Voice uppger i tillsynsärendet DI-2019-2488 att det per den 18 februari 2019 fanns 2,7 miljoner filer på lagringsservern Voice NAS, att dessa filer inte motsvarar 2,7 miljoner samtal, men att ett samtal motsvarar i genomsnitt cirka tre till fyra filer och att ett samtal kan utgöra upp till tio filer. IMY uppskattar utifrån genomsnittet antalet lagrade samtal i Voice NAS till mellan 650 000 och 900 000. Det är med andra ord frågan om ett mycket stort antal samtal.

Beträffande samtalens karaktär kan konstateras att de rör sjukvårdsrådgivning och att hälsouppgifterna är det centrala. Hälsouppgifter utgör känsliga personuppgifter enligt artikel 9 i dataskyddsförordningen och ställer höga krav på säkerheten för uppgifterna.

Behandling av personuppgifter inom hälso- och sjukvården innebär generellt en hög risk för de registrerades fri- och rättigheter.

Vården ska särskilt bygga på respekt för patientens självbestämmande och integritet, 5 kap. 1 § 3 HSL. Personuppgifter ska utformas och i övrigt behandlas så att patienters och övriga registrerades integritet respekteras samt ska dokumenterade personuppgifter hanteras och förvaras så att obehöriga inte får tillgång till dem, vilket framgår av artiklarna 5.1 f och 32 i dataskyddsförordningen samt av 1 kap. 2 § andra och tredje styckena PDL. Det finns även särskilt reglerat i HSLF-FS 2016:40 hur personuppgifter om patienter ska skyddas.

Alla som är sjuka har rätt att få tillgång till vård. Vårdsökande personer som ringer till 1177 får anses ha en hög förväntan på att obehöriga inte ska kunna ta del av uppgifter som förmedlas i ett samtal eftersom patienter har rätt till en konfidentiell och förtroendefull kontakt med vården. För privata vårdgivare regleras tystnadsplikten i 6 kap. 12–15 §§ PSL, som hälso- och sjukvårdspersonalen hos en privat vårdgivare ska följa.

Enligt artikel 32.1 i dataskyddsförordningen ska personuppgiftsansvarig vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken till skydd för de uppgifter som behandlas. Enligt artikel 32.2 ska vid bedömningen av lämplig säkerhetsnivå särskild hänsyn tas till de risker som behandlingen 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.

Förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystem och -tjänster är enligt artikel 32.1 b i dataskyddsförordningen en åtgärd som kan vara lämplig när det gäller att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. En annan åtgärd som kan vara lämplig när det gäller att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken är enligt artikel 32.1 d i dataskyddsförordningen ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Mot bakgrund av personuppgifternas känsliga karaktär, att personuppgifterna samlats in i ett förtroligt sammanhang som rör sjukvårdsrådgivning, behandlingens omfattning och behandlingens höga risker ställs enligt IMY:s uppfattning sammanfattningsvis höga krav på att vidta långtgående säkerhetsåtgärder enligt artikel 32.1 i dataskyddsförordningen. MedHelps ansvar omfattar även den lagring av personuppgifter om vårdsökande som skett i Voice NAS.

IMY konstaterar att ett stort antal samtal till 1177 som lagrats i Voice NAS exponerats mot internet under okänd tid utan skydd fram till den 18 februari 2019 då Voice vidtog åtgärder för att förhindra exponering mot internet. En exponering av personuppgifter mot internet utan skydd innebar att personuppgifterna var åtkomliga för alla som hade en internetuppkoppling. Det innebar en hög risk för obehörigt röjande av eller obehörig åtkomst till personuppgifterna.

MedHelp har uppgett att MedHelp inte kände till att personuppgifterna i Voice NAS blivit nåbara utan skyddsmekanismer, att det lagrade innehållet kom ut på nätet av okänd anledning för MedHelp och att MedHelp fick kännedom om personuppgiftsincidenten av Inera AB:s vice vd. IMY konstaterar att MedHelp agerat först efter incidenten genom att undersöka Voice NAS, föra över vårddokumentationen till egna servrar och ge Voice instruktion om radering av samtalen, vilket Voice utförde den 7 mars 2019.

IMY konstaterar mot denna bakgrund att MedHelp har saknat tillräcklig förmåga att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna. Enligt IMY har MedHelp även saknat ett verkkningsfullt förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

IMY konstaterar att det är frågan om många personuppgifter, som både är känsliga och föremål för tystnadsplikt, och att de exponerats mot internet utan skydd vilket inneburit de varit åtkomliga för alla som hade en internetuppkoppling. MedHelp har således inte skyddat personuppgifterna mot obehörigt röjande eller obehörig åtkomst och därmed inte iakttagit sin skyldighet som personuppgiftsansvarig att vidta lämpliga tekniska och organisatoriska åtgärder som säkerställt en säkerhetsnivå som är lämplig i förhållande till risken i enlighet med artikel 32.1 i dataskyddsförordningen.

Enligt den grundläggande säkerhetsprincipen i artikel 5.1 f i dataskyddsförordningen ska personuppgifter behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstörelse eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder. Att personuppgifterna har exponerats mot internet utan skydd mot obehörigt röjande eller obehörig åtkomst innebär enligt IMY att

bristen i säkerheten varit av sådant allvarligt slag att den även innebär en överträdelse av artikel 5.1 f i dataskyddsförordningen.

Skyldigheten att lämna information till vård sökande

IMY har den 25 juni 2019 tagit del av en utskrift från www.1177.se om 1177 sjukvårdsrådgivning på telefon. På webbsidan framgår att bakom 1177 Vårdguiden står den svenska sjukvården genom alla regioner i samverkan. 1177 är ett nationellt telefonnummer för sjukvårdsrådgivning som man kan ringa dygnet runt. Varje region driver sin egen verksamhet för sjukvårdsrådgivning antingen i egen regi eller genom upphandlad underleverantör. De samtal som är rådgivningssamtal journalförs. Frågan "Vem är ansvarig för att personuppgifterna hanteras rätt?" besvaras enligt följande. "Det är din vårdgivare som har ansvar för att personuppgifterna hanteras på ett korrekt och lagligt sätt. När vården ges av en region är det en eller flera styrelser i regionen som är ytterst ansvariga. Inom den privata vården är det företaget eller den verksamhet som bedriver vården som är ansvariga."

MedHelp uppgav bland annat följande vid inspektionen den 20 mars 2019. MedHelp mottar cirka 3 miljoner samtal per år inom ramen för 1177. Vilken information om personuppgiftsbehandling som ska lämnas och av vem regleras i avtalet med Hälso- och sjukvårdsförvaltningen, HSF (Region Stockholm, IMY:s anm.), som ansvarar för att informera de som ringer sjukvårdsupplysningen 1177. För några veckor sedan lämnades ingen information, men nu lämnas viss information. MedHelp har inte tillgängligt vilken information som ges i talsvaret. MedHelp kan inte rent praktiskt lämna information i talsvaret eftersom det är HSF som styr det. MedHelp representerar HSF och varumärket 1177, så MedHelp får inte säga till en person att denna har kommit till MedHelp. MedHelp lämnar information på sin hemsida om att MedHelp behandlar personuppgifter. Den 25 april 2019 uppger MedHelp att för Region Stockholm informeras den inringande om att samtalet kommer spelas in i patientsäkerhets- och kvalitetssyfte, att avtalet med Region Stockholm utgör ett offentligt upphandlat avtal där avtalsvillkoren således upprättats av regionen samt att som tjänsteleverantör till regionen är det inte möjligt för MedHelp att bestämma vilken information till registrerade som ska lämnas.

IMY:s bedömning

Den som är personuppgiftsansvarig ska enligt artikel 12.1 i dataskyddsförordningen vidta lämpliga åtgärder för att till den registrerade tillhandahålla all information enligt artiklarna 13 och 14 i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, i synnerhet för information som är särskilt riktad till barn. I artikel 13 anges vilken information som den personuppgiftsansvarige ska tillhandahålla om personuppgifterna samlas in från den registrerade.³ Den personuppgiftsansvarige ska enligt artikel 13.1 lämna information om bland annat identitet och kontaktuppgifter för den personuppgiftsansvarige, kontaktuppgifter för dataskyddsombudet i tillämpliga fall, ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen. Den personuppgiftsansvarige ska också enligt artikel 13.1 f lämna särskild information om denne avser att föra över personuppgifter till ett tredjeland.⁴

³ Artikel 14 i dataskyddsförordningen anger vilken information som den personuppgiftsansvarige ska tillhandahålla om personuppgifterna inte samlas in från den registrerade.

⁴ I tillämpliga fall information om att den personuppgiftsansvarige avser att överföra personuppgifter till ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artikel 46, 47 eller artikel 49.1 andra stycket, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.

Informationsskyldigheten är omfattande och en grundläggande förutsättning för att enskilda ska få kunskap om och kontroll över hur deras personuppgifter behandlas. Krav på öppenhet är en grundläggande princip enligt artikel 5.1 a i dataskyddsförordningen. Av skäl 60 i dataskyddsförordningen framgår att principerna om rättvis och öppen behandling fordrar att den registrerade informeras om att behandling sker och syftet med den. Den personuppgiftsansvarige bör till den registrerade lämna all ytterligare information som krävs för att säkerställa en rättvis och öppen behandling, med beaktande av personuppgiftsbehandlingens specifika omständigheter och sammanhang.

Information ska enligt artikel 13.2 lämnas bland annat om att det föreligger en rätt att av den personuppgiftsansvarige begära tillgång till personuppgifter. En vårdgivare ska också följa 8 kap. 6 § PDL som anger vilken information som vårdgivaren ska lämna till den registrerade utöver vad som framgår av artiklarna 13 och 14. Den informationen ska omfatta bland annat vad som gäller i fråga om sökbegrepp, direktåtkomst och utlämnande av uppgifter på medium för automatiserad behandling.

IMY konstaterar att det offentliga ansvaret för Region Stockholm som huvudman enligt HSL inte innebär någon bestämmanderätt över MedHelps dagliga verksamhet och det fråntar inte MedHelp ansvaret som följer med rollen som vårdgivare och personuppgiftsansvarig. Ansvarsskyldigheten i artikel 5.2 i dataskyddsförordningen innebär att det är MedHelp som ansvarar för och ska kunna visa att MedHelp efterlever de grundläggande dataskyddsprinciperna i artikel 5.1. Det är därmed MedHelp som har det yttersta ansvaret för att principen om öppenhet följs genom att vårdsökande får nödvändig information om personuppgiftsbehandlingen.

När en vårdsökande ringer 1177 samlar MedHelp som personuppgiftsansvarig vårdgivare in personuppgifter för ändamål som rör vårddokumentation. IMY konstaterar att det enligt artikel 13 i dataskyddsförordningen och 8 kap. 6 § PDL ställs omfattande krav på information som MedHelp inte lämnar. Det är inte tillräckligt att MedHelp i ett talsvarsmeddelande informerar vårdsökande om att samtalet kommer spelas in i patientsäkerhets- och kvalitetssyfte. Exempelvis saknas helt information om att MedHelp är personuppgiftsansvarig, om MedHelps kontaktuppgifter, om att personuppgifter samlas in för ändamål som rör vårddokumentation, om den rättsliga grunden för behandlingen samt om att det föreligger en rätt att av den personuppgiftsansvarige begära tillgång till personuppgifter. Det har också helt saknats information om att personuppgifter överförts till tredje land. Även den kompletterande information som krävs enligt 8 kap. 6 § PDL saknas.

Genom att MedHelp inte informerar vårdsökande i samband med insamlingen av personuppgifterna vid telefonsamtal till 1177, utöver ett talsvarsmeddelande att samtalet spelas in i patientsäkerhets- och kvalitetssyfte, konstaterar IMY att MedHelp har behandlat personuppgifter i strid med artikel 13 och det preciserade kravet på information till registrerade som framgår av 8 kap. 6 § PDL.

Av artikel 5.1 a i dataskyddsförordningen framgår att personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Avsaknaden av information enligt artikel 13 bedöms, eftersom den avsevärt begränsar vårdsökandes förutsättningar att ta tillvara sina rättigheter, vara så omfattande och så allvarig att bristen bedöms strida mot öppenhetsprincipen i artikel 5.1 a.

Ansvar för säkerhetskopiering

MedHelp uppger bland annat följande i tillsynsärendet. Inspelningen av samtal till 1177 som besvaras av MedHelps sjuksköterskor sker inom MedHelps egen telefoniplattform. Samtalen spelas in och lagras sedan på en lagringsserver. Det finns ingen säkerhetskopia på ljudfilerna. MedHelp har en speciallösning som ska hålla i många år utan säkerhetskopia. Filerna ligger på flera diskar i ett RAID-system. Så har lösningen alltid sett ut för MedHelps samtal. Inspelade samtal kan spelas upp av personal i MedHelps patientsäkerhetscentrum. I systemet kan det tas fram en träfflista och genom att klicka på en rad kan man komma vidare till journalanteckningen och spela upp samtalet.

IMY:s bedömning

Enligt artikel 32.1 i dataskyddsförordningen är personuppgiftsansvarig skyldig att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder. Enligt artikel 32.2 ska vid bedömningen av lämplig säkerhetsnivå särskild hänsyn tas till de risker som behandlingen 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. Förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident är enligt artikel 32.1 c en åtgärd som kan vara lämplig när det gäller att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

MedHelp behandlar inom sin telefoniplattform personuppgifter om vårdsökande i ljudfiler med inspelade samtal till 1177. Det sker i MedHelps verksamhet enligt HSL för ändamål som rör vårddokumentation. Personuppgifternas känsliga karaktär, att personuppgifterna samlats in i ett förtroligt sammanhang som rör sjukvårdsrådgivning, behandlingens omfattning och höga risker innebär högt ställda krav på de säkerhetsåtgärder som Medhelp ska vidta enligt artikel 32.1 i dataskyddsförordningen.

HSLF-FS 2016:40 innehåller uttryckliga föreskrifter om säkerhetskopiering. En vårdgivare ska enligt 3 kap. 12 § HSLF-FS 2016:40 säkerställa att personuppgifter som behandlas i informationssystem säkerhetskopieras med en fastställd periodicitet och att säkerhetskopiorna förvaras på ett säkert sätt, väl åtskilda från originaluppgifterna. Vårdgivaren ska även besluta om hur länge säkerhetskopiorna ska sparas och hur ofta återläsningstester av kopior ska göras, 3 kap.13 § HSLF-FS 2016:40. Socialstyrelsens föreskrifter utgör nationell rätt som kompletterar och preciserar dataskyddsförordningen och ställer ett uttryckligt krav på säkerhetskopiering. IMY konstaterar att säkerhetskopiering är en säkerhetsåtgärd som MedHelp ska vidta för att uppfylla kraven enligt artikel 32.1 i dataskyddsförordningen.

MedHelps användning av ett robust lagringsmedia, som exempelvis ett RAID-system, utgör inte säkerhetskopiering. Ett RAID-system erbjuder inte ett skydd som innebär att uppgifterna kan återskapas om det inträffar en incident som påverkar de lagrade uppgifternas riktighet, till exempel om systemet drabbas av skadlig kod. Att MedHelp använder ett RAID-system har däremot betydelse för MedHelps förmåga till kontinuitet i behandlingen, dvs. att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna på det sätt som framgår av artikel 32.1 b i dataskyddsförordningen.

Såväl åtgärder som vidtas för att säkerställa kontinuitet i den dagliga driften, till exempel genom att använda ett RAID-system, som åtgärder som vidtas för att kunna återgå till ordinarie drift efter en incident, till exempel säkerhetskopiering, är åtgärder

för att säkerställa tillgänglighet. Det innebär emellertid inte att dessa åtgärder kan ersätta varandra, utan att de kompletterar varandra.

IMY konstaterar att MedHelp, genom att inte säkerhetskopiera ljudfiler med inspelade samtal till 1177 inom MedHelps telefoniplattform, har behandlat personuppgifter i strid med artikel 32.1.

Enligt den grundläggande säkerhetsprincipen i artikel 5.1 f i dataskyddsförordningen ska personuppgifter behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstörelse eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder. Förlust av vårddokumentation kan innebära en hög risk för de vårdsökandes fri- och rättigheter. Underlåtenheten att genomföra säkerhetskopiering bedöms därför vara av så allvarigt slag att bristen även innebär en överträdelse av artikel 5.1 f i dataskyddsförordningen.

Val av ingripande

Möjliga ingripandeåtgärder

IMY har ett antal korrigerande befogenheter att tillgå enligt artikel 58.2 i dataskyddsförordningen, bland annat kan IMY förelägga den personuppgiftsansvarige att se till att behandlingen sker i enlighet med förordningen och om så krävs på ett specifikt sätt och inom en specifik period.

Enligt artiklarna 58.2 och 83.2 i dataskyddsförordningen har IMY befogenhet att påföra administrativa sanktionsavgifter i enlighet med artikel 83. Beroende på omständigheterna i det enskilda fallet ska administrativa sanktionsavgifter påföras utöver eller i stället för de andra åtgärder som avses i artikel 58.2. Vidare framgår av artikel 83.2 vilka faktorer som ska beaktas vid beslut om att administrativa sanktionsavgifter ska påföras och vid bestämmande av avgiftens storlek.

Om det är fråga om en mindre överträdelse får IMY enligt vad som anges i skäl 148 i dataskyddsförordningen i stället för att påföra en sanktionsavgift utfärda en reprimand enligt artikel 58.2 b i dataskyddsförordningen. Hänsyn ska tas till försvärande och förmildrande omständigheter i fallet, såsom överträdelsens karaktär, svårighetsgrad och varaktighet samt tidigare överträdelser av relevans.

Sanktionsavgift ska påföras

IMY har ovan bedömt att MedHelp har överträtt artiklarna 5.1 a och f, 6, 9, 13 och 32.1 i dataskyddsförordningen. Överträdelser av dessa artiklar kan enligt artikel 83.4 och 83.5 föranleda administrativa sanktionsavgifter.

Mot bakgrund av att de konstaterade överträdelserna har rört ett mycket stort antal vårdsökande som hänvisats att ringa 1177 för sjukvårdsrådgivning och har omfattat brister i hanteringen av känsliga personuppgifter såsom uppgifter om hälsa, är det inte frågan om mindre överträdelser.

Det finns således inte skäl att avseende någon av dessa överträdelser ersätta sanktionsavgiften med en reprimand. MedHelp ska därför påföras administrativa sanktionsavgifter.

Fastställande av sanktionsavgiftens storlek

Generella bestämmelser

Enligt artikel 83.1 i dataskyddsförordningen ska varje tillsynsmyndighet säkerställa att påförandet av administrativa sanktionsavgifter i varje enskilt fall är effektivt, proportionellt och avskräckande. I artikel 83.2 anges de faktorer som ska beaktas vid bestämmande av sanktionsavgiftens storlek gällande överträdelsen. Vid bedömningen av storleken på sanktionsavgiften ska hänsyn tas till bland annat överträdelsens karaktär, svårighetsgrad och varaktighet, om det varit frågan om uppsåt eller oaktsamhet, vilka åtgärder som vidtagits för att lindra den skada som de registrerade har lidit, graden av ansvar med beaktande av de tekniska och organisatoriska åtgärder som genomförts i enlighet med artiklarna 25 och 32, hur tillsynsobjektet har samarbetat med tillsynsmyndigheten, vilka kategorier av personuppgifter som berörs, hur överträdelsen kom till IMY:s kännedom och om det finns andra försvårande eller förmildrande faktorer, till exempel direkt eller indirekt ekonomisk vinst av förfarandet.

Överträdelser av artikel 5.1 a och f, 6, 9 och 13 i dataskyddsförordningen omfattas av den högre sanktionsavgiften enligt artikel 83.5. Sanktionsavgiften ska således bestämmas upp till 20 000 000 EUR eller, när det gäller ett företag, upp till fyra procent av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst för överträdelser rörande dessa artiklar. Överträdelser av artikel 32.1 omfattas av den lägre sanktionsavgiften enligt artikel 83.4. Sanktionsavgiften ska således bestämmas upp till 10 000 000 EUR eller, när det gäller ett företag, upp till två procent av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst för överträdelsen rörande denna artikel.

Begreppet "ett företag" omfattar alla företag som bedriver en ekonomisk verksamhet, oavsett enhetens juridiska status eller det sätt på vilket det finansieras.

Av skäl 150 i dataskyddsförordningen framgår bland annat att om administrativa sanktionsavgifter åläggs ett företag, bör ett företag anses vara ett företag i den mening som avses i artiklarna 101 och 102 i EUF-fördraget.

Detta innebär att bedömningen av vad som utgör ett företag ska utgå från konkurrensrättens definitioner. Reglerna för koncernansvar i EU:s konkurrenslagstiftning kretsar kring begreppet ekonomisk enhet. Ett moderbolag och ett dotterbolag betraktas som en del av samma ekonomiska enhet när moderbolaget utövar ett avgörande inflytande över dotterbolaget. Det avgörande inflytandet (dvs. kontrollen) kan antingen uppnås genom ägande eller genom avtal.

Av MedHelp AB:s årsredovisning framgår att MedHelp AB ingår i en koncern, där MedHelp AB ägs till 95 procent av MedHelp Group OY (ett finländskt aktiebolag) samt till 5 procent av Meddet AB.

IMY anser att det faktum att MedHelp ägs till 95 procent av MedHelp Group OY innebär att den aktuella koncernen ska anses vara en sådan ekonomisk enhet som avses inom konkurrensrätten. Enligt årsredovisningen för koncernen var årsomsättningen 223 013 000 kronor för räkenskapsåret 2019.⁵

⁵ Fyra procent av omsättningen motsvarar 8 920 000 kr och två procent 4 460 000 kr.

Det maximala beloppet för sanktionsavgifterna för överträdelser som omfattas av artikel 83.5 i dataskyddsförordningen är således 20 miljoner euro och för överträdelser som omfattas av artikel 83.4 10 miljoner euro.

Sanktionsavgift för respektive överträdelse

IMY har konstaterat fyra överträdelser som avser MedHelps personuppgiftsbehandling såsom personuppgiftsansvarig.

MedHelp har exponerat personuppgifter i form av ljudfiler med inspelade telefonsamtal till 1177 mot internet utan skydd mot obehörigt röjande av eller obehörig åtkomst till personuppgifterna i strid med artikel 5.1 f och artikel 32.1 i dataskyddsförordningen. MedHelp har behandlat personuppgifter genom att lämna ut känsliga personuppgifter till MediCall och låta MediCall samla in personuppgifter i strid med artikel 5.1 a, 6 och 9.1 i dataskyddsförordningen. MedHelp har inte tillhandahållit information till vårdsökande som ringt 1177 i strid med artikel 5.1 a och artikel 13 i dataskyddsförordningen. Slutligen har MedHelp inte säkerhetskopierat vårddokumentation i form av ljudfiler som innehåller inspelade samtal till 1177 som besvarats av MedHelps sjuksköterskor inom MedHelps telefoniplattform i strid med artikel 5.1 f och artikel 32.1 i dataskyddsförordningen.

IMY bedömer att de fyra överträdelserna inte utgör sammankopplade behandlingar och att det därför ska ges en sanktionsavgift per överträdelse.

För att sanktionsavgifter ska vara effektiva och avskräckande ska den personuppgiftsansvariges omsättning beaktas särskilt vid bestämmande av sanktionsavgifters storlek.⁶ En proportionalitetsbedömning måste också göras i varje enskilt fall. Vid proportionalitetsbedömningen får den sammanlagda sanktionsavgiften inte bli för hög i förhållande till de aktuella överträdelserna och inte heller för hög i förhållande till den som åläggs att betala sanktionsavgiften.

Sanktionsavgiften för respektive överträdelse fastställs enligt följande.

a) Behandling av personuppgifter om vårdsökande som MediCall utfört

MedHelp mottar cirka 3 miljoner samtal per år inom ramen för 1177, varav MediCall svarat på 20 procent. Det rör sig således om ca 600 000 samtal per år som MediCall besvarat. Det är försvårande att det är frågan om en omfattande behandling av känsliga och integritetskänsliga personuppgifter, att personuppgiftsbehandlingen utförts av en organisation som inte omfattas av de integritetsskyddande bestämmelser som gäller inom den svenska hälso- och sjukvården, t.ex. regleringen om tystnadsplikt, att vårdsökande inte har haft kännedom om att personuppgiftsbehandlingen har skett i Thailand samt att vårdsökande inte har kunnat avstå från den aktuella personuppgiftsbehandlingen.

Mot bakgrund av överträdelsernas allvar och att den administrativa sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande bestämmer IMY den administrativa sanktionsavgiften till 3 miljoner kronor för denna överträdelse.

b) Exponerade ljudfiler på lagringsservern Voice NAS

MedHelp har lagrat inspelningar av vårdsökandens samtal till 1177 på lagringsservern Voice NAS. Av utredningen framgår det att den 18 februari 2019 fanns 2,7 miljoner

⁶ Jämför med artiklarna 83.4 och 83.5 i dataskyddsförordningen.

filer på Voice NAS och att ett samtal motsvarar i genomsnitt cirka tre till fyra filer. IMY har mot den bakgrunden gjort uppskattningen att det rör sig om mellan 650 000 och 900 000 samtal.

Alla som är sjuka har rätt att få vård. Vårdsökande som inte är akut sjuka hänvisas till att ringa 1177. Det rör sig om en förtroendefull kontakt med vården där vårdsökande får anses ha en hög förväntan på att obehöriga inte ska få del av uppgifter som förmedlas under samtalet. Den som ringer kan inte motsätta sig att personuppgifter behandlas för ändamål som rör vårddokumentation.

Mot bakgrund av arten av uppgifterna och de högt ställda kraven på säkerhet för personuppgifter om vårdsökande är det en försvårande omständighet att MedHelp, såsom vårdgivare och personuppgiftsansvarig, har saknat kontroll över säkerheten för personuppgifterna. MedHelp kände inte till att personuppgifterna i Voice NAS blivit nåbara utan skyddsmekanismer. Det lagrade innehållet kom ut på nätet av okänd anledning för MedHelp. MedHelp fick kännedom om incidenten av Inera AB:s vice vd. MedHelp agerade först efter incidenten genom att undersöka Voice NAS, föra över vårddokumentationen till egna servrar och ge Voice besked om radering av samtalen.

Det är allvarligt att en stor mängd hälsouppgifter varit åtkomliga för alla som har en internetuppkoppling under okänd tid.

Mot bakgrund av överträdelsernas allvar och att den administrativa sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande bestämmer IMY den administrativa sanktionsavgiften till 8 miljoner kronor för denna överträdelse.

c) Information till vårdsökande

MedHelp mottar cirka 3 miljoner samtal per år inom ramen för 1177. Bestämmelserna om information innebär att MedHelp självmant ska göra vårdsökande personer medvetna om MedHelps personuppgiftsbehandling och deras rättigheter i samband med MedHelps behandling av personuppgifter. Det är frågan om en omfattande informationsplikt, som är grunden för att enskilda ska kunna ha kunskap om och kontroll över hur deras personuppgifter behandlas.

Det är försvårande att bristen på information rör ett stort antal vårdsökande och att det helt saknas information som motsvarar kraven enligt dataskyddsförordningen och PDL, utom såvitt avser ett talsvarsmeddelande om att samtalet kommer spelas in i patientsäkerhets- och kvalitetssyfte. Det förhållandet att information inte lämnas om bland annat att MedHelp är personuppgiftsansvarig, ändamålen och den rättsliga grunden för behandlingen och att vårdsökande kan vända sig till MedHelp för att utöva sina rättigheter enligt dataskyddsförordningen medför att förutsättningarna för vårdsökande att ta tillvara sina rättigheter begränsas avsevärt. MedHelp har även överfört personuppgifter om patienter till MediCall, ett thailändskt bolag. Det är försvårande att det helt saknats information om överföring av personuppgifter till Thailand, som är ett tredjeländ.

Mot bakgrund av överträdelsernas allvar och att den administrativa sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande bestämmer IMY den administrativa sanktionsavgiften till 500 000 kronor för denna överträdelse.

d) Säkerhetskopiering

MedHelp mottar cirka 3 miljoner samtal per år inom ramen för 1177. Avsaknad av säkerhetskopiering hos MedHelp rör således ett stort antal vårdsökanden. Det är en försvårande omständighet att det helt saknas säkerhetskopiering av vårddokumentation om ett stort antal vårdsökanden. Förlust av vårddokumentation kan innebära en hög risk för de vårdsökandes fri- och rättigheter.

Mot bakgrund av överträdelsernas allvar och att den administrativa sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande bestämmer IMY den administrativa sanktionsavgiften till 500 000 kronor för överträdelsen.

Sammanfattning

IMY har funnit att MedHelp ska betala en sammanlagd administrativ sanktionsavgift på 12 000 000 kronor för de konstaterade överträdelserna varav 3 000 000 kronor avser överträdelsen vid punkten a), 8 000 000 kronor avser överträdelsen vid punkten b), 500 000 kronor avser överträdelsen vid punkten c) och 500 000 kronor avser överträdelsen vid punkten d).

Förelägganden

MedHelp har inte informerat vårdsökande enligt kraven i dataskyddsförordningen och 8 kap. 6 § PDL. Bristen på information om bland annat vem som är personuppgiftsansvarig och dennes kontaktuppgifter begränsar vårdsökandens möjligheter att exempelvis kunna utöva rätten att begära tillgång till personuppgifter som MedHelp samlar in i samband med att vårdsökande ringer 1177. MedHelp har inte säkerhetskopierat ljudfiler som utgör vårddokumentation enligt dataskyddsförordningen och 3 kap. 12-13 §§ HSLF-FS 2016:40.

MedHelp mottar cirka 3 miljoner samtal per år inom ramen för 1177. Det är en stor mängd vårdsökande i behov av sjukvårdsrådgivning som påverkas av bristerna på information och säkerhetskopiering.

MedHelp ska därför föreläggas enligt artikel 58.2 d i dataskyddsförordningen att snarast och senast två månader efter det att beslutet vunnit laga kraft se till att behandlingen sker i enlighet med dataskyddsförordningen och kompletterande nationell rätt vad gäller information till vårdsökande och säkerhetskopiering.

MedHelp har anfört att MedHelp komma att lida ytterligare skada om eventuella förelägganden om information till registrerade och säkerhetskopiering är i konflikt med MedHelps avtal med Region Stockholm eller med upphandlingsrättslig lagstiftning. MedHelp har såsom vårdgivare och personuppgiftsansvarig det yttersta ansvaret för en laglig behandling av personuppgifter, vilket innefattar att vårdsökande får information om personuppgiftsbehandlingen och att åtgärder för säkerhetskopiering vidtas.

Detta beslut har fattats av generaldirektören Lena Lindgren Schelin efter föredragning av it-säkerhetsspecialisten Magnus Bergström och avdelningsdirektören Suzanne Isberg. I handläggningen har enhetschefen Katarina Tullstedt och juristen Mattias Sandström medverkat. Vid den slutliga handläggningen har även rättschefen David Törngren och enhetschefen Malin Blixt medverkat.

Lena Lindgren Schelin, 2021-06-07 (Det här är en elektronisk signatur)

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Integritetsskyddsmyndigheten. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär. Överklagandet ska ha kommit in till Integritetsskyddsmyndigheten senast tre veckor från den dag ni fick del av beslutet. Om överklagandet har kommit in i rätt tid sänder Integritetsskyddsmyndigheten det vidare till Förvaltningsrätten i Stockholm för prövning.

Ni kan e-posta överklagandet till Integritetsskyddsmyndigheten om det inte innehåller några integritetskänsliga personuppgifter eller uppgifter som kan omfattas av sekretess. Myndighetens kontaktuppgifter framgår av beslutets första sida.

Bilaga

Bilaga – Information om betalning av sanktionsavgift.

Kopia till

MedHelps vd via e-post