

Voice Integrate Nordic AB  
Färögatan 33  
164 53 Kista

**Diarienummer:**  
DI-2019-2488

**Ert diarienummer:**

**Datum:**  
2021-06-07

# Beslut efter tillsyn enligt dataskyddsförordningen mot Voice Integrate Nordic AB

## Innehåll

Integritetsskyddsmyndighetens beslut.....	2
Bakgrund.....	2
Motivering av beslutet.....	2
Rättslig bakgrund.....	2
Voice roll vid behandlingen av personuppgifterna.....	3
Uppgifter från Voice, MedHelp och Medical i incidentanmälningarna.....	3
Voice:s uppgifter i tillsynsärendet.....	3
IMY:s bedömning av Voice:s roll.....	4
Ansvaret för personuppgiftsincidenten i lagringsservern Voice NAS.....	5
Uppgifter från MedHelp, Medical och Voice i incidentanmälningarna.....	5
Uppgifter från Voice i tillsynsärendet.....	6
MedHelps uppgifter i tillsynsärendet DI-2019-3375.....	7
IMY:s bedömning.....	7
Val av ingripande.....	9
Möjliga ingripandeåtgärder.....	9
Sanktionsavgift ska påföras.....	10
Fastställande av sanktionsavgiftens storlek.....	10
Generella bestämmelser.....	10
Bedömning av förmildrande och försvårande omständigheter.....	11
Hur man överklagar.....	12

**Postadress:**  
Box 8114  
104 20 Stockholm

**Webbplats:**  
[www.imy.se](http://www.imy.se)

**E-post:**  
[imy@imy.se](mailto:imy@imy.se)

**Telefon:**  
08-657 61 00

## Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten (IMY) konstaterar att Voice Integrate Nordic AB (Voice) såsom personuppgiftsbiträde från okänt datum fram till den 18 februari 2019 i lagringsservern Voice NAS har exponerat personuppgifter i ljudfiler med inspelade telefonsamtal till 1177<sup>1</sup> mot internet utan skydd mot obehörigt röjande av eller obehörig åtkomst till personuppgifterna. Voice har därigenom i strid med artikel 32.1 i dataskyddsförordningen<sup>2</sup> underlåtit att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå för uppgifterna.

IMY beslutar med stöd av artikel 58.2 och 83 i dataskyddsförordningen att Voice ska betala en administrativ sanktionsavgift på 650 000 (sexhundrafemtio tusen) kronor för överträdelse av artikel 32.1 i dataskyddsförordningen.

## 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 Voice och genomförde en inspektion hos Voice den 6 mars 2019 för att kontrollera hur Voice behandlade personuppgifter inom ramen för 1177.

IMY inledde även tillsyn mot Inera AB och MedHelp AB (MedHelp). 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

Personuppgiftsansvarig definieras som 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, artikel 4.7 i dataskyddsförordningen. Enligt 2 kap. 6 patientdatalagen (2008:355), PDL, är en vårdgivare personuppgiftsansvarig för behandling av personuppgifter som vårdgivaren utför i verksamhet enligt exempelvis hälso- och sjukvårdslagen (2017:30), HSL, bland annat vid behandling av personuppgifter för ändamål som rör vårddokumentation enligt 2 kap. 4 § första stycket 1 och 2 PDL. I 3 kap. PDL regleras skyldigheten att föra patientjournal.

<sup>1</sup> På webbplatsen 1177.se anges "Ring telefonnummer 1177 för sjukvårdsrådgivning dygnet runt."

<sup>2</sup> 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).

Ett personuppgiftsbiträde är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning, artikel 4.8 i dataskyddsförordningen.

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.

## **Voice roll vid behandlingen av personuppgifterna**

### **Uppgifter från Voice, MedHelp och Medical i incidentanmälningarna**

I anmälan av en personuppgiftsincident den 21 februari 2019 (IMY:s ärende PUI-2019-705) uppger Voice bland annat att Voice är personuppgiftsansvarig och att ett säkerhetshål i en lagringsserver upptäcktes av Computer Sweden som publicerat denna information i sin tidning.

IMY mottog den 20 februari 2019 MedHelps anmälan av en personuppgiftsincident (IMY:s ärende PUI-2019-689). I anmälan uppger MedHelp att Voice och MediCall är personuppgiftsbiträde. MedHelp uppger i tillsynsärendet DI-2019-3375 att MedHelp har anlitat MediCall som underleverantör för sjukvårdsrådgivning via telefon när enskilda ringer 1177.

IMY mottog den 21 februari 2019 MediCalls anmälan av en personuppgiftsincident (IMY:s ärende PUI-2019-698) i vilken incidenten beskrivs som "Intrång i underleverantörs (Voice Integrate Nordic ab) server." Efter att IMY ställt frågor till MediCall uppger MediCall den 19 juni 2019 bland annat att samtalen spelades in av Biz och lagrades hos Voice på uppdrag av MedHelp.

### **Voice:s uppgifter i tillsynsärendet**

Voice har uppgett bland annat följande i detta tillsynsärende.

Voice är ett utvecklingsbolag som tar fram programvara. Ingen anställd har legitimation inom hälso- och sjukvården. Voice är inte personuppgiftsansvarig i dataskyddsförordningens mening. Anmälan av en personuppgiftsincident har getts in för att vara på den säkra sidan. Voice har inte heller varit personuppgiftsbiträde i dataskyddsförordningens mening.

Det uppstår ett samtalsflöde när en person ringer till 1177. De inspelade samtalen är samtal från personer som ringt 1177 och sedan kopplats vidare till MedHelp och MediCall. Genom att lyssna på filerna kan man höra vad inringande säger, som exempelvis namn, adress och vad man vill ha hjälp med. Voice uppdrag i 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.

Voice och MedHelp har ingått Leveransavtal – tjänster, som är daterat och undertecknat den 1 september 2012, där det framgår att Voice och MedHelp sedan många år har haft ett tätt samarbete inom teknik, säkerhet och möjliga förbättringar inom både teknik, tjänster samt produktion. Avtalet beskriver tjänster och omfattning som bland annat "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 och därefter årsvis till dess endera part säger upp avtalet.

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.

Bilaga 1 till "Personuppgiftsbiträdesavtal" innehåller instruktioner till personuppgiftsbiträdet. Av instruktionen framgår bland annat följande. Om syfte och ändamål i punkt 3 att "Leverantören ska för MedHelps räkning Behandla de Personuppgifter som är nödvändiga för att Leverantören ska kunna uppfylla sina förpliktelser i enlighet med Tjänsteavtal och för att MedHelp ska kunna leverera tjänster till MedHelps kunder och partners i enlighet med Kundavtal." Om kategorier av personuppgifter i punkt 5 framgår att de personuppgifter som behandlas avser bland andra "hälsodata".

Voice stängde ner 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 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 är idag okänt för Voice.

På IMY:s fråga den 14 mars 2019 om det fanns några samtalsfiler kvar på Voice NAS har Voice uppgett att samtalen hade raderats på begäran av MedHelp den 7 mars 2019.

#### **IMY:s bedömning av Voice:s roll**

Voice har i tillsynsärendet uppgivit att de varken är personuppgiftsansvariga eller personuppgiftsbiträde i dataskyddsförordningens mening. Här konstateras att det är de faktiska omständigheterna som avgör vilken roll en aktör har vid behandling av personuppgifter.

Voice har inte legitimerad hälso- och sjukvårdspersonal anställd. I ärendet har inte framkommit någon annan omständighet som innebär att Voice bedriver verksamhet enligt HSL och därmed skulle ha en skyldighet att föra patientjournal enligt 3 kap. PDL och skulle vara en personuppgiftsansvarig vårdgivare enligt 2 kap. 6 § PDL. Det har inte heller i övrigt framkommit omständigheter som innebär att Voice ska betraktas som personuppgiftsansvarig enligt artikel 4.7 i dataskyddsförordningen.

Däremot behandlade Voice personuppgifter för MedHelps räkning.

Voice har med MedHelp ingått Leveransavtal – tjänster och Personuppgiftsbiträdesavtal med tillhörande instruktion, som omfattar inspelning av samtal, sjukvårdsrådgivning och hälsodata. Voice behandlade inspelade samtal från enskilda som ringt 1177 i lagringsservern Voice NAS när incidenten upptäcktes den 18 februari 2019 och Voice stängde ner lagringsservern och ändrade så att servern inte längre var nåbar via internet genom att ip-tables infördes.

Voice har även gett MedHelp tillgång till Voice NAS den 20 februari 2019 och senare den 7 mars 2019 raderat uppgifterna på MedHelps begäran. MedHelp uppger i anmälan av personuppgiftsincident att Voice är personuppgiftsbiträde. MediCall uppger i ärendet om anmälan av en personuppgiftsincident att den rör "Intrång i underleverantörs (Voice Integrate Nordic ab) server." samt att samtalen spelades in av Biz och lagrades av Voice på uppdrag av MedHelp.

IMY konstaterar att Voice genom att spela in och lagra ljudfiler med personuppgifter i form av telefonsamtal till 1177 i lagringsservern Voice NAS, i vart fall fram till den 7 mars 2019, har varit personuppgiftsbiträde för MedHelp enligt definitionen i artikel 4.8 i dataskyddsförordningen.

## **Ansvaret för personuppgiftsincidenten i lagringsservern Voice NAS**

### **Uppgifter från MedHelp, Mediacall 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.

I MediCalls anmälan av en personuppgiftsincident beskrivs incidenten 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 av Voice på uppdrag av MedHelp.

I Voice:s anmälan av personuppgiftsincident beskrivs incidenten 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

Voice har uppgett bland annat följande i detta tillsynsärende.

Voice stängde ned lagringsservern den 18 februari 2019 och ändrade så att servern inte längre var nåbar via internet genom att ip-tables 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.

Syftet med Voice NAS var att hantera och lagra Voice interna filer, inte att hantera kunders datafiler. Den incident som föranlett tillsynsärendet hos IMY ägde rum på en "passiv" server. Med "passiv" avses Voice egen lagringsserver, vilken passivt tog emot datafiler. Inga inloggningskonton fanns. Voice interna server hade ett säkerhetscertifikat som aktiverats mot en publik ip-adress samt en publik domän. På grund av en felkonfigurering hade lagringsservern blivit "aktiv" och kunde därmed nås utanför callcentersystemet via ett säkerhetshål i programvaran, Apache webbserver. I samband därmed har servern också tillåtit kommunikation via okrypterad http istället, för som avsett, bara tillåta https.

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

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 för inspelning av samtal. Det är riktigt att datafiler med inspelade samtal kommit att överföras från MedHelp till lagringsservern 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.

I "Personuppgiftsbiträdesavtal", som undertecknades av MedHelp den 7 maj 2018 och av Voice den 10 maj 2018 framgår av punkt 11 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.

Av instruktionen i Bilaga 1 till "Personuppgiftsbiträdesavtal" framgår bland annat följande. Punkt 7 om informationssäkerhet innehåller bland annat att "Leverantören har en rutin för att identifiera hot och risker, avseende informationssäkerhet och Behandling av Personuppgifter, inom verksamheten och inom varje enskilt informationssystem." och att "Leverantörens informationssäkerhetsarbete innefattar säkerhet beträffande informationstillgångar rörande förmågan att upprätthålla konfidentialitet." Som ett exempel på krav som leverantören minst ska uppfylla finns "Begränsad extern åtkomst" som innebär att "Leverantören ska tillse att Leverantörens datasystem är skyddade från extern åtkomst genom tekniska lösningar såsom brandvägg och inloggningskontroll vid extern åtkomst via Internet eller modem."

### **MedHelps uppgifter i tillsynsärendet DI-2019-3375**

MedHelp har uppgett bland annat följande i tillsynsärendet.

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. 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.

### **IMY:s bedömning**

Ljudfilerna i lagringsservern Voice NAS hos Voice innehöll inspelade samtal till 1177 i samband med sjukvårdsrådgivning. Såsom konstateras ovan är Voice personuppgiftsbiträde för behandlingen av dessa personuppgifter. Av "Leveransavtal – tjänster" samt "Personuppgiftsbiträdesavtal" och den tillhörande instruktionen framgår att uppdraget till Voice innefattade bland annat inspelning av samtal, sjukvårdsrådgivning och hälsodata.

Behandlingen av personuppgifterna har ägt rum hos Voice i verksamhet där Voice åtagit sig att leverera tjänster och där Voice är personuppgiftsbiträde. Voice har därvid också ansvaret för säkerheten i samband med behandlingen enligt artikel 32 i dataskyddsförordningen.

Voice måste därför i egenskap av personuppgiftsbiträde 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.

MedHelp uppger i tillsynsärendet DI-2019-3375 att 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 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 artikel 32 i dataskyddsförordningen samt av 1 kap. 2 § andra och tredje styckena PDL.

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. Hälso- och sjukvårdspersonal som tar emot dessa telefonsamtal omfattas vanligen av bestämmelser om tystnadsplikt i 6 kap. 12–15 §§ patientsäkerhetslagen (2010:659) samt i offentlighets- och sekretesslagen (2009:400).

Enligt artikel 32.1 i dataskyddsförordningen ska ett personuppgiftsbiträde 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 överförs, 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.

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. En exponering av personuppgifter mot internet utan skydd innebär att personuppgifterna var åtkomliga för alla som hade en internetuppkoppling. Det innebär en hög risk för obehörigt röjande av eller obehörig åtkomst till personuppgifterna.

Voice:s ansvar omfattar skyddet för den lagring av personuppgifter om vårdsökande som skett i Voice NAS och att säkerställa säkerheten för uppgifterna genom lämpliga tekniska och organisatoriska åtgärder. Uppgifterna har exponerats mot internet helt utan skydd och Voice har uppgett att Voice fick kännedom om personuppgiftsincidenten genom en artikel i Computer Sweden.

IMY konstaterar mot denna bakgrund att Voice har saknat tillräcklig förmåga att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna. Enligt IMY har Voice 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 ett mycket stort antal personuppgifter, som både är känsliga och föremål för tystnadsplikt inom hälso- och sjukvården, och att personuppgifter exponerats mot internet helt utan skydd vilket inneburit de varit åtkomliga för alla som hade en internetuppkoppling. Voice har således inte skyddat personuppgifterna mot obehörigt röjande eller obehörig åtkomst och därmed inte iakttagit sin skyldighet som personuppgiftsbiträde 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

## Val av ingripande

### Möjliga ingripandeåtgärder

IMY har ett antal korrigerande befogenheter att tillgå enligt artikel 58.2 i dataskyddsförordningen, bland annat att förelägga personuppgiftsbiträdet 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 framgår att IMY kan 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 konstaterat att Voice har överträtt artikel 32.1 i dataskyddsförordningen i samband med behandlingen av de personuppgifter som omfattades av personuppgiftsincidenten. Denna artikel omfattas av artikel 83.4 och vid en sådan överträdelse ska tillsynsmyndigheten överväga att påföra administrativ sanktionsavgift utöver, eller i stället för, andra korrigerande åtgärder.

Mot bakgrund av att den konstaterade överträdelsen har rört ett mycket stort antal vård sökande som hänvisats att ringa 1177 för sjukvårdsrådgivning samt omfattat brister i hantering av känsliga och integritetskänsliga personuppgifter såsom uppgifter om hälsa, är det inte frågan om en mindre överträdelse.

Det finns således inte skäl att ersätta sanktionsavgiften med en reprimand. Voice 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.

Överträdelse 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.

För att sanktionsavgifter ska vara effektiva och avskräckande ska den personuppgiftsansvariges omsättning beaktas särskilt vid bestämmande av sanktionsavgiftens storlek.<sup>3</sup> 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.

Av årsredovisningen för räkenskapsåret 2019 framgår att Voice hade en omsättning om 5 889 000 kr.

<sup>3</sup> Jämför med artiklarna 83.4 i dataskyddsförordningen.

**Bedömning av förmildrande och försvårande omständigheter**

IMY har konstaterat att Voice 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 32.1 i dataskyddsförordningen.

Voice 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 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.

Mot bakgrund av arten av uppgifterna, att det är frågan om känsliga personuppgifter som omfattas av tystnadsplikt, och de högt ställda kraven på säkerhet för personuppgifter om vårdsökande, är det en försvårande omständighet att Voice såsom personuppgiftsbiträde har saknat kontroll över säkerheten för personuppgifterna. Voice kände inte till att personuppgifterna i Voice NAS blivit nåbara helt utan skyddsmekanismer och fick kännedom om personuppgiftsincidenten genom en artikel i Computer Sweden.

Det är allvarligt att en stor mängd hälsouppgifter exponerats utan skydd och därigenom varit åtkomliga för alla som har en internetuppkoppling under okänd tid.

IMY kan konstatera att Voice agerat direkt när Voice fick kännedom om personuppgiftsincidenten, men att detta inte påverkar bedömningen av incidentens allvarlighet i sig.

Mot bakgrund av överträdelsernas allvar och att den administrativa sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande bestämmer IMY den administrativa sanktionsavgiften till 650 000 kronor för överträdelsen av artikel 32.1 i dataskyddsförordningen.

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**

Voice Integrate Nordic ABs vd via e-post.