Voice Integrate Nordic AB

Färögatan 33

164 53 Kista

Record number:

DI-2019-2488

Your record number:

Date:

2021-06-07

Decision after supervision according to

the Data Protection Regulation against Voice

Integrate Nordic AB

Content

Postal address:

Box 8114

104 20 Stockholm

Website:

www.imy.se

E-mail:

imy@imy.se

Phone:

08-657 61 00

The decision of the Integrity Protection Authority

The Swedish Privacy Protection Authority (IMY) states that Voice Integrate Nordic AB (Voice)

as a personal data assistant from an unknown date until 18 February 2019 in

the Voice NAS storage server has exposed personal data in audio files with recorded

telephone call to 11771 against the Internet without protection against unauthorized disclosure of or unauthorized

access to personal data. Voice thereby infringes Article 32 (1) of the

the Data Protection Regulation2 has failed to take appropriate technical and organizational measures

measures to ensure an appropriate level of security for the data.

In accordance with Article 58 (2) and 83 of the Data Protection Regulation, the IMY decides that Voice shall:

pay an administrative sanction fee of 650,000 (six hundred and fifty thousand) kronor for

infringement of Article 32 (1) of the Data Protection Regulation.

Background

On February 18, 2019, Computer Sweden published an article entitled “2.7

million recorded calls to 1177 Vårdguiden completely unprotected on the internet ”. In the article

states, among other things, that “On an open web server, completely without password protection or

other security, we have found 2.7 million recorded calls to the advisory number 1177. "

IMY initiated supervision of Voice and conducted an inspection at Voice on March 6

2019 to check how Voice processed personal data within the framework of 1177.

IMY also initiated supervision of Inera AB and MedHelp AB (MedHelp). It turned out that

three regions hired MedHelp as a care provider when care seekers call 1177 for

healthcare advice and partly Inera AB to connect the calls to MedHelp. IMY

therefore initiated supervision against the Health and Medical Care Board Region Stockholm,

Regional Board Region Sörmland and Regional Board Region Värmland.

Justification of the decision

Legal background

The person responsible for personal data is defined as a natural or legal person, publicly

authority, institution or other body as alone or together with others

determines the purposes and means of processing personal data; if

the purposes and means of processing are determined by Union law or

national law of the Member States, the controller or the specific

the criteria for its designation are laid down in Union law or in that of the Member States

national law, Article 4 (7) of the Data Protection Regulation. According to ch. 6 Patient Data Act

(2008: 355), PDL, is a care provider responsible for the processing of personal data

personal data that the care provider performs in activities according to, for example, health and

the Health Care Act (2017: 30), HSL, among other things when processing personal data for

purposes relating to care documentation according to ch. § 4 first paragraph 1 and 2 PDL. I 3

Cape. PDL regulates the obligation to keep a patient record.

The website 1177.se states "Call telephone number 1177 for medical advice around the clock.".

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the

natural persons with regard to the processing of personal data and on the free movement of such data and on

repeal of Directive 95/46 / EC (General Data Protection Regulation).

1

2

Integrity Protection Authority

Registration number: DI-2019-2488

Date: 2021-06-07

3 (12)

A personal data assistant is a natural or legal person, public authority,

institution or other body that processes personal data for it

on behalf of data controllers, Article 4 (8) of the Data Protection Regulation.

According to Article 32 (1) of the Data Protection Regulation, both the personal data controller shall:

and the personal data assistant take appropriate technical and organizational measures to:

ensure an appropriate level of security to protect the data being processed. At

the assessment of the appropriate technical and organizational measures

the personal data controller and the personal data assistant take into account the latest developments,

implementation costs and the nature, scope, context and nature of the treatment;

purposes and the risks to the rights and freedoms of natural persons. According to Article 32 (1)

include appropriate safeguards, where appropriate; (a) pseudonymisation; and

encryption of personal data, b) the ability to continuously ensure confidentiality,
integrity, availability and resilience of treatment systems and services,
c) the ability to restore the availability and access to personal data in a reasonable time
in the event of a physical or technical incident, and (d) a procedure for regular testing;
examine and evaluate the effectiveness of the technical and organizational measures
which will ensure the safety of the treatment.

According to Article 32 (2) of the Data Protection Regulation, in the assessment of appropriate
safety level special consideration is given to the risks posed by the treatment, in particular
for unintentional or unlawful destruction, loss or alteration or for unauthorized disclosure of
or unauthorized access to the personal data transferred, stored or otherwise
treated.

Voice role in the processing of personal data

Information from Voice, MedHelp and Medicall in the incident reports

In the report of a personal data incident on 21 February 2019 (IMY's case PUI-2019705), Voice states, among other things,
that Voice is responsible for personal data and that a
security holes in a storage server were discovered by Computer Sweden as published
this information in his newspaper.

On 20 February 2019, IMY received MedHelp's report of a personal data incident
(IMY case PUI-2019-689). In the notification, MedHelp states that Voice and MediCall are
personal data assistant. MedHelp states in the supervisory case DI-2019-3375 that MedHelp
has hired MediCall as a subcontractor for healthcare advice by telephone when
individual caller 1177.

On 21 February 2019, IMY received MediCall's report of a personal data incident
(IMY's case PUI-2019-698) in which the incident is described as “Intrusion in
subcontractor (Voice Integrate Nordic ab) server. ” After the IMY asked questions
MediCall states on 19 June 2019, among other things, that the calls were recorded by

Biz and stored at Voice on behalf of MedHelp.

Voice's tasks in the supervisory matter

Voice has stated, among other things, the following in this supervisory matter.

Voice is a development company that develops software. No employee has identification

in health care. Voice is not responsible for personal data in

meaning of the Data Protection Regulation. Reporting of a personal data incident has been submitted

to be on the safe side. Voice has also not been a personal data assistant in

meaning of the Data Protection Regulation.

A call flow occurs when a person calls 1177. The recorded calls are

calls from people who called 1177 and then connected to MedHelp and

MediCall. By listening to the files, you can hear what callers are saying, like

for example, name, address and what you want help with. Voice assignment in agreement with

MedHelp and MediCall have been delivering calls via their exchanges and providing support for

features and software covered by the agreement. Voice has produced

Biz software.

Voice and MedHelp have entered into Delivery Agreements - services, which are dated and

signed on September 1, 2012, stating that Voice and MedHelp then

for many years has had a close collaboration in technology, security and possible improvements

in both technology, services and production. The agreement describes services and scope

such as "Recording (within system) CC-50," Recording calls ",

"Search functions for retrieval" and "Filtering or deleting recordings according to

customer's wishes ”. The delivery agreement applies from 2012-09-01 t.o.m. 2019-06-30 and

thereafter annually until either party terminates the agreement.

An agreement called the "Personal Data Assistant Agreement" was signed by MedHelp on 7 May 2018 and by Voice on May 10, 2018. Voice is referred to as the supplier in the agreement, which includes the following. MedHelp has entered into agreements with customers and partners for example regarding an agreement that MedHelp shall provide healthcare advice to customers and partners. The agreement regulates the MedHelp Group's handover of personal data to the supplier in connection with service agreements and other agreements entered into between MedHelp and the provider.

Appendix 1 to the "Personal Data Assistant Agreement" contains instructions for the personal data assistant. The instructions state, among other things, the following. About purpose and purpose in paragraph 3 that “The Supplier shall, on behalf of MedHelp, Process the Personal information that is necessary for the Supplier to be able to fulfill its obligations in accordance with the Service Agreement and for MedHelp to be able to deliver services to MedHelp's customers and partners in accordance with Customer Agreements. ” About categories of personal data in paragraph 5 it appears that the personal data processed refers to among other "health data".

Voice shut down the storage server on February 18, 2019 and changed that server was no longer reachable via the internet by ip-tables (a firewall tool to allow or block network access) was introduced directly into the server. After In the incident, MedHelp wanted IT forensics to investigate Voice NAS. MedHelp was therefore granted permission to enter Voice NAS on February 20, 2019. MedHelp is also said to have started moving the content of Voice NAS to MedHelp's own servers. If the transfer of the data took place by simply copying the files or because the files were deleted in connection with the copying is currently unknown to Voice.

On IMY's question on March 14, 2019 if there were any call files left on Voice NAS Voice stated that the calls had been deleted at the request of MedHelp on 7 March

2019.

IMY's assessment of Voice's role

In the supervisory case, Voice has stated that they are neither responsible for personal data nor personal data assistant within the meaning of the Data Protection Regulation. Here it is stated that they are the facts that determine the role of an actor in dealing with personal data.

Voice does not employ licensed health care professionals. In the case has not has emerged another circumstance which means that Voice conducts business according to HSL and thus would have an obligation to keep a patient record according to ch. PDL and would be a care provider responsible for personal data according to ch. 6 § PDL. It has nor have circumstances otherwise emerged which mean that Voice must be considered as data controller in accordance with Article 4 (7) of the Data Protection Regulation.

However, Voice processed personal data on behalf of MedHelp.

Voice has entered into a Delivery Agreement with MedHelp - services and Personal data assistant agreement with accompanying instructions, which includes recording of calls, healthcare advice and health data. Voice processed recorded calls from individuals who called 1177 in the storage server Voice NAS when the incident was discovered on the 18th February 2019 and Voice shut down the storage server and changed so that the server does not was no longer accessible via the internet with the introduction of ip-tables.

Voice has also given MedHelp access to Voice NAS on February 20, 2019 and later on March 7, 2019, deleted the information at MedHelp's request. MedHelp states in notification of personal data incident that Voice is a personal data assistant. MediCall

states in the case of reporting a personal data incident that it concerns “Intrusion in

subcontractor (Voice Integrate Nordic ab) server. ” and that the conversations were recorded by

Biz and stored by Voice on behalf of MedHelp.

IMY states that Voice by recording and storing audio files with personal data in

in the form of telephone calls to 1177 in the storage server Voice NAS, at least until the 7th

March 2019, has been a personal data assistant for MedHelp as defined in Article 4 (8) i

the Data Protection Regulation.

Responsibility for the personal data incident in the Voice storage server

NAS

Information from MedHelp, Medicall and Voice in the incident reports

In MedHelp's report of a personal data incident, the incident is described as being sensitive

personal data had been exposed to the internet without any safeguards and that

an unknown number of audio files have been available. The incident concerns patients and employees of it

subcontractor of the data controller. Personal data covered by

the incident is stated to be health, sexual life, social security number, date of birth, identifying

information, such as first and last name and contact information. Furthermore, it appears that

MedHelp became aware of the personal data incident by Inera AB's Deputy CEO.

MediCall's report of a personal data incident describes the incident as “Intrusion in

subcontractor (Voice Integrate Nordic ab) server. ” The incident concerns patients.

Personal information covered by the incident is stated to be health, social security number and

identifying information, such as first and last name. After the IMY asked questions

MediCall stated on 19 June 2019, among other things, that the calls were stored off

Voice on behalf of MedHelp.

In Voice's report of a personal data incident, the incident is described as a

security holes in a storage server were discovered by Computer Sweden who published

this information in an article. The incident concerns patients and business users in minor

extent. Personal data covered by the incident is stated to be health,

social security number, identifying information such as first and last name and

contact information.

Information from Voice in the supervisory matter

Voice has stated, among other things, the following in this supervisory matter.

Voice shut down the storage server on February 18, 2019 and changed that server

was no longer accessible via the internet by introducing ip-tables directly into the server.

After the incident came to light, MedHelp wanted IT forensics to investigate

the Voice NAS storage server. MedHelp was therefore granted permission to access Voice NAS

on February 20, 2019. MedHelp is also said to have started moving the content of Voice NAS to

MedHelp's own servers. If the transfer of the data took place by simply copying

the files or by deleting the files during copying were unknown to Voice.

Voice has stated on IMY's question on March 14, 2019, if there were any conversation files

left on Voice NAS, that the calls had been deleted at the request of MedHelp on March 7

2019.

The purpose of Voice NAS was to manage and store Voice internal files, not to manage

customer data files. The incident that prompted the supervisory case at IMY took place on one

"Passive" server. "Passive" refers to Voice's own storage server, which passively received

data files. There were no login accounts. Voice internal server had one

security certificate activated against a public IP address and a public domain. On

due to a misconfiguration, the storage server had become "active" and could thus be accessed

outside the call center system through a security hole in the software, the Apache web server. IN

in connection with this, the server has also allowed communication via unencrypted http instead,

for as intended, only allow https.

A call flow occurs when a person calls 1177. The recorded calls are

calls from people who called 1177 and then connected to MedHelp and

MediCall. As of February 18, 2019, there were 2.7 million files on the Voice storage server

NAS, that these files do not correspond to 2.7 million calls, but that one call corresponds to

on average about three to four files and that a call can be up to ten files.

Voice assignments according to agreements with MedHelp and MediCall have been to deliver calls via

their switches and provide support for functions and software covered by the agreement.

Voice has developed the Biz software for recording calls. It is true that

data files with recorded calls have been transferred from MedHelp to the storage server

Voice NAS, a networked storage device. It has been prompted by Medhelps

own server had crashed. Medhelp's server problem started already in 2013 to

then escalate and lead to an emergency situation in the fall of 2015. Voice management did not participate in

this decision or enforced it, but became aware that the files were there on the 18th

February 2019 when the incident attracted media attention.

No recordings would have been stored at Voice. One month before

The Data Protection Regulation was to enter into force, MedHelp suddenly sent over one

personal data assistant agreement. Such a thing had not previously existed between the parties.

The agreement was presented as a standard agreement that all parties to the agreement needed to enter into

that the Data Protection Regulation entered into force.

In the "Personal Data Assistant Agreement", which was signed by MedHelp on 7 May 2018 and

of Voice on 10 May 2018, it appears from point 11, among other things, that a party must continuously during

during the contract period, carry out a check that the information security work is in accordance

with laws and regulations in force at any given time, which means, among other things, that a party must

carry out internal audits, safeguards and risk analyzes.

The instructions in Appendix 1 to the "Personal Data Assistant Agreement" state, among other things following. Point 7 on information security contains, among other things, that “The Supplier has a routine for identifying threats and risks, regarding information security and Processing of Personal Data, within the business and within each individual information system. " and that “The Supplier's information security work includes security of information resources regarding the ability to maintain confidentiality. " As an example of requirements that the supplier must at least meet is available "Limited external access" which means that the Supplier shall ensure that the Supplier's computer systems are protected from external access by technical solutions such as firewall and login control for external access via Internet or modem. "

MedHelp's information in the supervisory matter DI-2019-3375

MedHelp has stated, among other things, the following in the supervisory matter.

MedHelp knew that MediCall stored calls with Voice, but MedHelp did not know that the server has been made accessible without protection mechanisms from the internet. Medicall's nurses was connected to Medhelp's network from 23 February 2019, instead of to the telephony solution Biz at Voice. This meant that the calls that were dialed were redirected to Medhelps servers and infrastructure, including to Collab which is a telephony solution that Assist the operations themselves.

MedHelp receives approximately 3 million calls per year within the framework of 1177. Eighty percent of these are handled by MedHelp and twenty percent are handled by Medicall, as before used the IT solution Biz which includes audio file storage. For a reason unknown to MedHelp the stored content then came online. Then the calls could not be stored at

Voice longer, they were transferred to MedHelp's servers. MedHelp's storage devices never have crashed. MedHelp did not have any server issues that led to an emergency autumn 2015. There has never been any transfer of data files with recorded patient calls from MedHelp to Voice. MedHelp has always stored recordings of patient calls exclusively in-house on own storage units. Voice has never stored recordings commissioned by MedHelp. However, Voice has stored recordings of patient calls on behalf of MedHelp's subcontractor MediCall.

IMY's assessment

The audio files in the Voice NAS storage server at Voice contained recorded calls to 1177 i in connection with healthcare advice. As noted above is Voice personal data assistant for the processing of this personal data. By "Delivery agreement - services ”and the“ Personal Data Assistant Agreement ”and the associated instructions appear that the assignment to Voice included, among other things, recording of conversations, health care advice and health data.

The processing of personal data has taken place at Voice in operations where Voice undertook to deliver services and where Voice is the personal data assistant. Voice has that also the responsibility for the security of the processing under Article 32 i the Data Protection Regulation.

Voice must therefore, as a personal data assistant, take appropriate technical and organizational measures to ensure an appropriate level of security in relation to the risk. In assessing the appropriate level of safety, special consideration shall be given taken to the risks posed by the treatment, in particular from unintentional or illegal destruction, loss or alteration or to unauthorized disclosure of or unauthorized access to the personal data transferred, stored or otherwise processed, Article 32 (1)

and 2 of the Data Protection Regulation. Ensuring adequate security means that

must adapt the level of safety to the risks of the treatment in question.

In supervisory case DI-2019-3375, MedHelp states that Medicall's treatment concerned 20

percent of the approximately 3 million telephone calls that MedHelp received annually via 1177,

a total of about 600,000 calls per year.

Voice states in the supervisory case that as of February 18, 2019, there were 2.7 million files

on the Voice NAS storage server, that these files do not correspond to 2.7 million calls, however

that a call corresponds to an average of about three to four files and that a call can constitute

up to ten files. Based on the average, IMY estimates the number of calls stored in Voice NAS

to between 650,000 and 900,000. In other words, it is a question of a very large number

Call.

Regarding the nature of the conversations, it can be stated that they concern health care counseling and that

health information is central. Health data constitute sensitive personal data according to

Article 9 of the Data Protection Regulation and places high demands on the security of the data.

Processing of personal data in health care generally means a high

risk to the data subjects' freedoms and rights.

Care should be based in particular on respect for the patient's self-determination and integrity,

Chapter 5 1 § 3 HSL. Personal data must be designed and otherwise processed so that

patients 'and other data subjects' integrity is respected and must be documented

personal data is handled and stored so that unauthorized persons do not have access to them, which

appears from Article 32 of the Data Protection Ordinance and from ch. § 2 second and third

the pieces PDL.

Everyone who is ill has the right to access care. Care seekers who call

1177 may be considered to have a high expectation that unauthorized persons will not be able to access information

conveyed in a conversation because patients have the right to a confidential and
trusting contact with healthcare. Healthcare professionals who receive these
Telephone calls are usually covered by provisions on professional secrecy in Chapter 6. §§ 12–15
the Patient Safety Act (2010: 659) and the Public Access to Information and Secrecy Act (2009: 400).
According to Article 32 (1) of the Data Protection Regulation, a personal data assistant shall take
appropriate technical and organizational measures to ensure a level of security
which is appropriate in relation to the risk of protection of the data being processed. According to
Article 32 (2), when assessing the appropriate level of safety, special consideration shall be given to:
risks posed by the treatment, in particular from accidental or unlawful destruction;
loss or alteration or to unauthorized disclosure of or unauthorized access to the
personal data transferred, stored or otherwise processed.
The ability to continuously ensure confidentiality, integrity, availability and
resilience of treatment systems and services is in accordance with Article 32 (1) (b) (i)
the Data Protection Regulation is a measure that may be appropriate in terms of ensuring
a level of safety appropriate to the risk. Another action that can
be appropriate in ensuring a level of safety that is appropriate in relation
to risk is, in accordance with Article 32 (1) (d) of the Data Protection Regulation, a procedure for:
regularly test, examine and evaluate the effectiveness of the technical and
organizational measures to ensure the safety of treatment.
Integrity Protection Authority
Registration number: DI-2019-2488
Date: 2021-06-07
9 (12)
In view of the sensitive nature of the personal data, that the personal data has been collected
into a confidential context related to healthcare counseling, the scope of treatment
and the high risks of treatment are, in IMY's view, summarized

high requirements for far-reaching safety measures in accordance with Article 32 (1) (i)
the Data Protection Regulation.

IMY notes that a large number of calls to 1177 stored in Voice NAS have been exposed
against the internet for an unknown period of time without protection until 18 February 2019. An exposure
of personal data against the Internet without protection meant that the personal data was
accessible to anyone who had an internet connection. This entailed a high risk
unauthorized disclosure of or unauthorized access to personal data.

Voice's responsibilities include the protection of the storage of personal data about care seekers
done in Voice NAS and to ensure the security of the data through appropriate
technical and organizational measures. The information has been exposed to the internet completely
without protection and Voice has stated that Voice became aware of
the personal data incident through an article in Computer Sweden.

Against this background, the IMY notes that Voice has lacked sufficient capacity to
continuously ensure the confidentiality, integrity, availability and resilience of
treatment systems and services. According to IMY, Voice has also been missing one
effective procedure for regularly testing, examining and evaluating
the effectiveness of the technical and organizational measures to be ensured
the safety of treatment.

IMY states that it is a question of a very large number of personal data, as both
are sensitive and subject to professional secrecy in health care, and that
personal data has been exposed to the internet completely without protection, which has meant that they have been
accessible to anyone who had an internet connection. Voice has thus not protected
the personal data against unauthorized touching or unauthorized access and thus not
complied with his obligation as a personal data assistant to take appropriate technical and
organizational measures that ensure an appropriate level of security in relation
to the risk in accordance with Article 32 (1) of the Data Protection Regulation

Choice of intervention

Possible intervention measures

The IMY has a number of remedial powers available under Article 58 (2) (i)
the Data Protection Regulation, including instructing the personal data assistant to ensure that
processing takes place in accordance with the Regulation and if required in a specific way
and within a specific period.

According to Articles 58 (2) and 83 (2) of the Data Protection Regulation, the IMY can:
impose administrative penalty charges in accordance with Article 83
the circumstances of the individual case, administrative penalty fees shall be imposed
in addition to or in place of the other measures referred to in Article 58 (2). Furthermore, it appears from
Article 83 (2), the factors to be taken into account when deciding whether to
penalty fees shall be imposed and in determining the size of the fee.

In the case of a minor infringement, the IMY may, in accordance with recital 148 of the
instead of imposing a penalty fee, issue a reprimand
pursuant to Article 58 (2) (b) of the Data Protection Regulation. Account must be taken of aggravating and

mitigating circumstances in the case, such as the nature of the infringement, the degree of difficulty
and duration as well as previous violations of relevance.

A penalty fee must be imposed

IMY has stated above that Voice has infringed Article 32 (1) of the Data Protection Regulation in
in connection with the processing of the personal data covered by
the personal data incident. This Article is covered by Article 83 (4) and in the case of such
infringement, the supervisory authority shall consider imposing an administrative penalty fee

in addition to, or instead of, other corrective actions.

In view of the fact that the infringement found has affected a very large number
care seekers who have been referred to call 1177 for health care advice and covered
shortcomings in the handling of sensitive and privacy-sensitive personal data such as data
on health, it is not a matter of a minor violation.

There is thus no reason to replace the sanction fee with a reprimand. Voice ska
therefore, administrative penalty fees are imposed.

Determining the size of the penalty fee

General provisions

Pursuant to Article 83 (1) of the Data Protection Regulation, each supervisory authority shall ensure that:
the imposition of administrative penalty charges in each individual case is effective;
proportionate and dissuasive. Article 83 (2) sets out the factors to be taken into account in
determining the amount of the penalty fee applicable to the infringement. In the assessment
of the size of the penalty fee, account shall be taken of, among other things, the infringement
character, degree of difficulty and duration, whether it was a matter of intent or
negligence, what measures have been taken to alleviate the damage they registered
has suffered, the degree of responsibility taking into account the technical and organizational measures
carried out in accordance with Articles 25 and 32, the nature of the supervised entity
cooperated with the supervisory authority, the categories of personal data concerned;
how the infringement came to the IMY's knowledge and whether there are other aggravators or
mitigating factors, such as direct or indirect financial gain from the proceeding.

Infringement of Article 32 (1) is subject to the lower penalty fee provided for in Article 83 (4).
The penalty fee must therefore be set at up to EUR 10 000 000 or, in the case of
a company, up to two percent of total global annual sales during
previous financial year, depending on the maximum value of the infringement
this article.

In order for penalty fees to be effective and dissuasive, it must

the turnover of the data controller is taken into account in particular when determining

size of penalty fees.3 A proportionality assessment must also be made in each

individual case. In the proportionality assessment, the total penalty fee is received

does not become too high in relation to the current infringements nor does it become too high in

in relation to the person who is ordered to pay the penalty fee.

The annual report for the financial year 2019 shows that Voice had sales

about DKK 5,889,000.

3

Compare with Article 83 (4) of the Data Protection Regulation.

Assessment of mitigating and aggravating circumstances

IMY has stated that Voice has exposed personal data in the form of audio files with

recorded telephone calls to 1177 against the Internet without protection against unauthorized disclosure of or

unauthorized access to personal data in violation of Article 32 (1) (i)

the Data Protection Regulation.

Voice has stored recordings of the care applicant's calls to 1177 on the storage server

Voice NAS. The investigation shows that on 18 February 2019 there were 2.7 million

files on Voice NAS and that a call corresponds to an average of about three to four files. IMY

Against this background, it has been estimated that it is between 650,000 and

900,000 calls.

Everyone who is ill has the right to receive care. Care seekers who are not acutely ill are referred to

to call 1177. This is a trusting contact with the care where the care seeker

may be considered to have a high expectation that unauthorized persons will not receive information such as conveyed during the conversation.

Given the nature of the data, that it is a matter of sensitive personal data covered by the obligation of professional secrecy, and the high security requirements for personal information about care seekers, it is an aggravating circumstance that Voice such as personal data assistant has lacked control over the security of personal data.

Voice did not know that the personal data in Voice NAS had become completely accessible without protection mechanisms and became aware of the personal data incident through an article in Computer Sweden.

It is serious that a large amount of health information has been exposed without protection and thereby being accessible to anyone who has an internet connection for an unknown period of time.

IMY can state that Voice acted immediately when Voice became aware of the personal data incident, but that this does not affect the assessment of the incident severity per se.

In view of the seriousness of the infringements and the administrative penalty fee shall be effective, proportionate and dissuasive, the IMY determines the administrative the penalty fee of SEK 650,000 for the violation of Article 32 (1) i the Data Protection Regulation.

This decision was made by Director General Lena Lindgren Schelin after the presentation by the IT security specialist Magnus Bergström and the department director Suzanne Iceberg. In the proceedings, the unit manager Katarina Tullstedt and the lawyer Mattias Sandström participated. At the final hearing, the Chief Justice also has David Törngren and unit manager Malin Blixt participated.

Lena Lindgren Schelin, 2021-06-07 (This is an electronic signature)

How to appeal

If you want to appeal the decision, you must write to the Privacy Protection Authority. Enter i

the letter which decision you are appealing and the change you are requesting. The appeal shall

have been received by the Privacy Protection Authority no later than three weeks from the day you received

part of the decision. If the appeal has been received in time, send

The Integrity Protection Authority forwards it to the Administrative Court in Stockholm

examination.

You can e-mail the appeal to the Privacy Protection Authority if it does not contain

any privacy-sensitive personal data or data that may be covered by

secrecy. The authority's contact information can be found on the first page of the decision.

Appendix

Appendix - Information on payment of penalty fee.

Copy to

Voice Integrate Nordic ABs CEO via email.