Voice Integrate Nordic AB

Färögatan 33

164 53 Coffin

Diary number:

DI-2019-2488

Your diary number:

Date:

2021-06-07

Decision after supervision according to

data protection regulation against Voice

Integrate Nordic AB

Content

Mailing address:

Box 8114

104 20 Stockholm

Website:

www.imy.se

E-mail:

imy@imy.se

Phone:

08-657 61 00

The Privacy Protection Authority's decision

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

as personal data assistant from an unknown date until February 18, 2019 i

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

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

access to the personal data. Voice has thereby contravened Article 32.1 i

the data protection regulation2 failed to take appropriate technical and organizational measures

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

IMY decides with the support of article 58.2 and 83 of the data protection regulation that Voice shall

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

violation of Article 32.1 of the Data Protection Regulation.

Background

On February 18, 2019, Computer Sweden published an article with the title "2.7

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

is stated, 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 advice number 1177."

The IMY commenced supervision of Voice and carried out an inspection at Voice on 6 March

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 appeared 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 of the Health and Medical Board Region Stockholm,

The Regional Board Region Sörmland and the Regional Board Region Värmland.

Justification of the decision

Legal background

Personal data controller is defined as a natural or legal person, public

authority, institution or other body alone or together with others

determines the purposes and means of the processing of personal data; if

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

the national law of the Member States can the personal data controller or the special

the criteria for how he is to be appointed are prescribed in Union law or in the Member States

national law, Article 4.7 of the Data Protection Regulation. According to ch. 2 6 of the Patient Data Act

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

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

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

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

Cape. PDL regulated the obligation to keep patient records.

On the website 1177.se it is stated "Call telephone number 1177 for healthcare advice around the clock.".

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

of

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

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

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

institution or other body that processes personal data for it

account of the personal data controller, Article 4.8 of the data protection regulation.

According to article 32.1 of the data protection regulation, both the personal data controller must

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

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

the assessment of which technical and organizational measures are appropriate must

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

the implementation costs and the nature, extent, context and

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 the treatment systems and services,
c) the ability to restore availability and access to personal data in a reasonable time
in the event of a physical or technical incident, and d) a procedure to regularly test,
investigate and evaluate the effectiveness of the technical and organizational measures
which must ensure the safety of the treatment.

According to article 32.2 of the data protection regulation, when assessing the appropriate
security level special consideration is given to the risks that the treatment entails, in particular
for accidental or unlawful destruction, loss or alteration or for unauthorized disclosure of
or unauthorized access to the personal data transmitted, stored or otherwise
treated.

Voice role in the processing of personal data

Information from Voice, MedHelp and Medicall in the incident reports

In the notification of a personal data incident on 21 February 2019 (IMY's case PUI-2019705), Voice states, among other things, that Voice is the personal data controller and that a
security hole in a storage server was discovered by Computer Sweden as published
this information in their paper.

On February 20, 2019, IMY received MedHelp's notification of a personal data incident
(IMY case PUI-2019-689). In the report, 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 via telephone when
individuals call 1177.

On 21 February 2019, IMY received MediCall's notification of a personal data incident
(IMY's case PUI-2019-698) in which the incident is described as "Infringement of
subcontractor's (Voice Integrate Nordic ab) server." After IMY asked questions to

MediCall states on June 19, 2019, among other things, that the calls were recorded by

Biz and was stored with 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 produces software. No employee has identification

within health care. Voice is not responsible for personal data

meaning of the data protection regulation. The notification of a personal data incident has been submitted

to be on the safe side. Voice has also not been a personal data processor 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 were then connected to MedHelp and

MediCall. By listening to the files, one can hear what the caller is saying, such as

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 as well as providing support for

functions and software covered by the agreement. Voice has developed

the software Biz.

Voice and MedHelp have entered into a Supply Agreement – Services, which is dated and

signed on September 1, 2012, which states that Voice and MedHelp then

many years have had a close collaboration in technology, safety and possible improvements

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

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

“Retrieval search functions” and “Filtering or removing recordings according to

customer's wishes". The delivery agreement applies from 2012-09-01 up to and including 2019-06-30 and thereafter annually until either party terminates the agreement.

An agreement named "Personal Data Processor Agreement" was signed by MedHelp on 7 May 2018 and by Voice on May 10, 2018. Voice is named as the supplier in the agreement, where, among other things, the following appears. MedHelp has entered into agreements with customers and partners for example as regards an agreement that MedHelp shall provide healthcare advice to customers and partners. The agreement regulates the MedHelp Group's transfer of personal data to the supplier due to service contracts and other agreements entered into between MedHelp and the supplier.

Appendix 1 to the "Personal data service agreement" contains instructions for the personal data assistant. The instruction states, among other things, the following. About purpose and purpose in point 3 that "The Supplier shall, on MedHelp's behalf, Treat the Personal data 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 the Customer Agreement." About categories of personal data in point 5 it is clear that the personal data that is processed refers to other "health data".

Voice shut down the storage server on February 18, 2019 and changed the 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 incident was brought to attention, MedHelp wanted IT forensics to examine Voice NAS. MedHelp was therefore granted access to Voice NAS on February 20, 2019.

MedHelp has also started to transfer the content of the Voice NAS to MedHelp's own servers. If the transfer of the data took place by merely copying the files or by the fact that the files were removed in connection with the copying is today unknown to Voice.

On IMY's question on March 14, 2019 if there were any call files left on the Voice NAS

the Voice stated that the calls had been deleted at the request of MedHelp on March 7

2019.

IMY's assessment of Voice's role

Voice has stated in the supervisory matter that they are neither responsible for personal data nor

personal data assistant in the sense of the data protection regulation. Here it is established that they are

factual circumstances that determine what role an actor has in the treatment of

personal data.

Voice does not employ licensed healthcare professionals. In the case did not

any other circumstance has emerged which means that Voice is conducting business

according to HSL and thus would have an obligation to keep patient records according to ch. 3. PDL

and would be a care provider responsible for personal data according to ch. 2 § 6 PDL. It has

nor otherwise have circumstances emerged which mean that Voice should be considered

as a personal data controller according to 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 associated 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 18

February 2019 and Voice shut down the storage server and changed so that the server does not

longer was reachable via the internet by introducing ip-tables.

Voice has also given MedHelp access to Voice NAS on February 20, 2019 and later

on March 7, 2019 deleted the data at MedHelp's request. MedHelp states in

notification of a personal data incident that Voice is a personal data assistant. MediCall states in the case of notification of a personal data incident that it relates to "Breach of subcontractor's (Voice Integrate Nordic ab) server." and that the conversations were recorded by Biz and was stored by Voice on behalf of MedHelp.

IMY states that Voice by recording and storing audio files with personal data in form of phone call to 1177 in the storage server Voice NAS, at least until the 7th March 2019, has been personal data assistant for MedHelp as defined in article 4.8 i data protection regulation.

Responsibility for the personal data incident in the storage server Voice NAS

Data from MedHelp, Medicall and Voice in the incident reports

In MedHelp's notification of a personal data incident, the incident is described as sensitive personal data had been exposed to the internet without any protection mechanisms and that an unknown number of audio files have been available. The incident concerns patients and employees of it the personal data controller's subcontractor. Personal data covered by the incident is stated to be health, sex life, social security number, date of birth, identifying information, for example first and last name and contact information. Furthermore, it appears that MedHelp was made aware of the personal data incident by Inera AB's vice president.

In MediCall's notification of a personal data incident, the incident is described as "Breach of subcontractor's (Voice Integrate Nordic ab) server." The incident concerns patients. Personal data covered by the incident are listed as health, social security number and identifying information, such as first and last name. After IMY asked questions to MediCall stated on June 19, 2019, among other things, that the calls were stored by Voice on behalf of MedHelp.

In Voice's notification of a personal data incident, the incident is described as a security hole in a storage server was discovered by Computer Sweden who published

this information in an article. The incident affects patients and business users to a lesser extent

extent. Personal data covered by the incident are listed as health,

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

contact information.

Data 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 the server

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

After the incident was brought to attention, MedHelp wanted IT forensics to investigate

the Voice NAS storage server. MedHelp was therefore given permission to enter Voice NAS

on February 20, 2019. MedHelp should also have started to transfer the content of the Voice NAS to

MedHelp's own servers. If the data was moved by copying only

the files or by the files being deleted in connection with the copying was unknown to Voice.

Voice has stated on IMY's question on March 14, 2019, if there were any call 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 led to the supervisory case at IMY took place on a

"passive" server. By "passive" is meant Voice's own storage server, which passively received

data files. No login accounts were found. 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 via 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,

because 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 are 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 i

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

Voice assignment according to the agreement with MedHelp and MediCall has been to deliver calls via

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

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

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

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

own server had crashed. Medhelp's server problems started back in 2013 because

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

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

February 2019 when the incident was noticed in the media.

No recordings would have been stored with Voice. A month before

the data protection regulation was to come into effect, MedHelp suddenly sent over one

personal data processing agreement. Nothing like this had previously existed between the parties.

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

that the data protection regulation entered into force.

In the “Personal Data Processor Agreement”, which was signed by MedHelp on May 7, 2018 and

by Voice on 10 May 2018, point 11 states, among other things, that the party must continuously under

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

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

From the instructions in Appendix 1 to the "Personal data service agreement" it appears, 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 regarding information assets relating to the ability to maintain confidentiality." As an example of requirements that the supplier must at least fulfill is available "Limited external access" which means that "The Supplier must ensure that the Supplier's computer systems are protected from external access through technical solutions such as firewall and login control for external access via the Internet or modem."

MedHelp's data in the supervisory case 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 that the server was 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 made were redirected to Medhelps servers and infrastructure, including to Collab which is a telephony solution that Medhelp themselves operate.

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 reasons unknown to MedHelp

the stored content then came out online. As 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 problems that led to an emergency situation
autumn 2015. There has never been any transfer of data files with recorded
patient calls from MedHelp to Voice. MedHelp has at all times stored recordings of
patient calls exclusively under own authority on own storage devices. Voice has never stored
recordings on behalf of 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
connection with healthcare advice. As noted above, Voice is
personal data officer for the processing of this personal data. Of "Delivery agreement -
services" and "Personal data service agreement" and the associated instructions appear
that the mission to Voice included, among other things, recording of calls,
healthcare advice and health data.

The processing of the personal data has taken place at Voice in operations where Voice
committed to delivering services and where Voice is a personal data processor. Voice has thereby
also the responsibility for security in connection with the processing according to Article 32 i
data protection regulation.

Voice must therefore, in its capacity as a personal data processor, take appropriate technical and
organizational measures to ensure a level of security that is appropriate i
relation to the risk. When assessing the appropriate security level, special consideration must be given
taken to the risks that the processing entails, in particular from accidental 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 one

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

MedHelp states in the supervisory case DI-2019-3375 that Medicall's treatment concerned 20

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

a total of approx. 600,000 calls per year.

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

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

that a call corresponds on average to around three to four files and that a call can constitute

up to ten files. IMY estimates based on the average the number of calls stored in the 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 relate to healthcare advice and that

the health information is central. Health information constitutes sensitive personal data according to

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

Processing of personal data in healthcare generally means a lot

risk to the freedoms and rights of the data subjects.

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

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

the privacy of patients and other data subjects is respected and must be documented

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

appears from article 32 of the data protection regulation and from ch. 1 § 2 second and third

the paragraphs PDL.

Everyone who is ill has the right to access care. Persons seeking care who call

1177 may be considered to have a high expectation that unauthorized persons should not be able to access information which is conveyed in a conversation because patients have a right to a confidential and trusting contact with care. Healthcare professionals who receive these telephone calls are usually covered by provisions on confidentiality in ch. 6. Sections 12–15 the Patient Safety Act (2010:659) and in the Publicity and Confidentiality Act (2009:400).

According to article 32.1 of the data protection regulation, a personal data assistant must take appropriate technical and organizational measures to ensure a level of security which is appropriate in relation to the risk to the protection of the data being processed. According to Article 32.2 must be taken into account when assessing the appropriate level of security risks that the processing entails, in particular from accidental or illegal destruction, loss or alteration or to unauthorized disclosure of or unauthorized access to them personal data transferred, stored or otherwise processed.

The ability to continuously ensure confidentiality, integrity, availability and resilience of treatment systems and services is according to Article 32.1 b i the data protection regulation a measure that may be appropriate when it comes to ensuring a level of security that is appropriate in relation to the risk. Another action that can be appropriate in ensuring a level of safety that is appropriate in relation to the risk is, according to Article 32.1 d of the data protection regulation, a procedure to regularly test, investigate and evaluate the effectiveness of the technical and organizational measures to ensure the safety of the treatment.

In light of the sensitive nature of the personal data, that the personal data has been collected into a confidential context relating to healthcare advice, the extent of the treatment

and the high risks of the treatment are posed according to IMY's opinion in summary high requirements to take far-reaching security measures according to Article 32.1 i 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 February 18, 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. That meant a high risk of unauthorized disclosure of or unauthorized access to the personal data.

Voice's responsibility includes the protection of the storage of personal data about care seekers that took place in Voice NAS and to ensure the security of the data through appropriate technical and organizational measures. The data 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, IMY states that Voice has lacked sufficient ability to continuously ensure the confidentiality, integrity, availability and resilience of the treatment systems and services. According to IMY, Voice has also lacked one effective procedure for regularly testing, investigating and evaluating the effectiveness of the technical and organizational measures to ensure the safety of the treatment.

IMY states that it is a question of a very large number of personal data, which both are sensitive and subject to a duty of confidentiality within the health care system, and that personal data exposed to the internet completely without protection, which meant they were accessible to anyone who had an internet connection. Voice has thus not protected the personal data against unauthorized handling or unauthorized access and thus not observed its obligation as personal data assistant to take appropriate technical and organizational measures that ensure a level of security that is appropriate 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 corrective powers available under Article 58.2 i

the data protection regulation, including instructing the personal data assistant to ensure that

the 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 protection regulation, it appears that IMY can

impose administrative penalty fees in accordance with Article 83. Subject to

the circumstances of the individual case, administrative penalty fees must be imposed

in addition to or instead of the other measures referred to in Article 58.2. Furthermore, it appears from

article 83.2 which factors must be taken into account when deciding whether administrative

penalty fees must be imposed and when determining the size of the fee.

If it is a question of a minor violation, IMY receives according to what is stated in reason 148 i

data protection regulation instead of imposing a penalty charge issue a reprimand

according to article 58.2 b of the data protection regulation. Consideration shall be given to aggravating and

mitigating circumstances of the case, such as the nature of the violation, degree of severity

and duration as well as previous violations of relevance.

A penalty fee must be imposed

IMY has stated above that Voice has violated Article 32.1 of the Data Protection Ordinance i

in connection with the processing of the personal data covered

the personal data incident. This article is covered by article 83.4 and in such case

violation, the supervisory authority shall consider imposing an administrative penalty fee in addition to, or in lieu of, other corrective actions.

In light of the fact that the established violation has affected a very large number care seekers who have been referred to call 1177 for healthcare advice and covered deficiencies in the handling of sensitive and privacy-sensitive personal data such as data on health, it is not a question of a minor transgression.

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

Determining the size of the penalty fee

General provisions

According to Article 83.1 of the Data Protection Regulation, each supervisory authority must ensure that the imposition of administrative penalty charges on a case-by-case basis is effective; proportionate and dissuasive. Article 83.2 specifies the factors to be taken into account when determining the size of the penalty fee for the violation. At the assessment of the size of the penalty fee, account must be taken of, among other things, the violation nature, severity and duration, whether it was a matter of intent or negligence, what steps were taken to mitigate the damage they recorded has suffered, the degree of responsibility taking into account the technical and organizational measures carried out in accordance with articles 25 and 32, how the subject of supervision has cooperated with the supervisory authority, which categories of personal data are affected, how the violation came to IMY's attention and whether there are other aggravating circumstances or mitigating factors, for example direct or indirect financial gain from the procedure.

Violation of Article 32.1 is covered by the lower penalty fee according to Article 83.4.

The penalty fee shall thus be determined up to EUR 10,000,000 or, where applicable a company, up to two percent of the total global annual turnover during previous budget year, depending on which value is the highest for the violation in question

this article.

For penalty fees to be effective and dissuasive, they must

the personal data controller's turnover 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 given

does not become too high in relation to the violations in question and also not too high i

relation to the person ordered to pay the penalty fee.

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

about SEK 5,889,000.

3

Compare with articles 83.4 of the data protection regulation.

Assessment of mitigating and aggravating circumstances

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

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

unauthorized access to the personal data in violation of Article 32.1 i

data protection regulation.

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

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

files on the Voice NAS and that one call corresponds on average to about three to four files. IMY

against that background has made the estimate that it is between 650,000 and

900,000 calls.

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

to call 1177. This involves a trusting contact with the care where care seekers

may be considered to have a high expectation that unauthorized persons should not have access to information that

conveyed during the conversation.

In light of the nature of the data, that it is a matter of sensitive personal data

which is subject to confidentiality, and the high security requirements for

personal data about care seekers, it is an aggravating circumstance that Voice such as

personal data controller has lacked control over the security of the personal data.

Voice did not know that the personal data in the Voice NAS had become completely accessible

protection mechanisms and became aware of the personal data incident through an article i

Computer Sweden.

It is serious that a large amount of health data was exposed without protection and

thereby being accessible to anyone with an internet connection for an unknown amount 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

seriousness in itself.

In light of the seriousness of the violations and that the administrative penalty fee

must be effective, proportionate and dissuasive, IMY determines the administrative

the penalty fee of SEK 650,000 for the violation of Article 32.1 i

data protection regulation.

This decision has been taken by the general manager Lena Lindgren Schelin after a presentation

by IT security specialist Magnus Bergström and department director Suzanne

Iceberg. In the handling are the unit manager Katarina Tullstedt and the lawyer Mattias

Sandström participated. In the final proceedings, the Chief Justice David also has

Törngren and unit manager Malin Blixt participated.

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

The Swedish Privacy Protection Authority

How to appeal

If you want to appeal the decision, you must write to the Swedish Privacy Agency. Enter in 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 it part of the decision. If the appeal has been received in time, send The Privacy 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 information that may be covered by secrecy. The authority's contact details appear on the first page of the decision.

Appendix

Appendix – Information on payment of penalty fee.

Copy to

Voice Integrate Nordic AB's CEO via e-mail.