MedHelp AB

Marieviksgatan 19

117 43 Stockholm

Record number:

DI-2019-3375

Your record number:

Date:

2021-06-07

Decision after supervision according to

the Data Protection Regulation against

MedHelp 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

As a care provider responsible for personal data according to ch. Section 6 of the Patient Data Act (2008: 355), PDL, MedHelp AB (MedHelp) has processed personal data about care seekers in violation of the Data Protection Regulation1 in the following way.

a)

Medhelp has during the period from 25 May 2018 to 31 August 2019 by disclose personal information to the Thai company MediCall and let MediCall collects personal data processed personal data in violation of Articles 5 (1) (a), 6 and 9 (1) of the Data Protection Regulation.

b)

Medhelp has from unknown date until 18 February 2019 in the storage server Voice NAS exposed personal data in audio files with recorded phone calls to 11772 against the Internet without protection against unauthorized disclosure or unauthorized use access to personal data. MedHelp thereby has in conflict with the articles 5.1 f and 32.1 of the Data Protection Regulation have failed to take appropriate technical measures and organizational measures to ensure an appropriate level of security for the data.

c)

At the time of the inspection on March 20, 2019, Medhelp has, in addition to one voicemail message that the call is being recorded in patient safety and

quality purpose, not informed care seekers about the company

personal data processing in connection with the collection of personal data at

telephone call to 1177. MedHelp has thereby processed personal data in

in violation of Articles 5 (1) (a) and 13 of the Data Protection Regulation.

d)

At the time of the inspection on March 20, 2019, Medhelp did not

backed up audio files with recorded calls to 1177 answered by

MedHelp's nurses within MedHelp's telephony platform. MedHelp has

thereby processed personal data in breach of Articles 5 (1) (f) and 32 (1) (i)

the Data Protection Regulation.

The Privacy Protection Agency (IMY) decides on the basis of Articles 58 (2) and 83 of the

the Data Protection Ordinance that MedHelp must pay an administrative penalty fee of

SEK 12,000,000 (twelve million) for the violations as follows. 3,000,000 (three

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).

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

million) refers to point a), SEK 8,000,000 (eight million) refers to point b),

SEK 500,000 (five hundred thousand) refers to point c) and SEK 500,000 (five hundred thousand)

kronor refers to point d).

In accordance with Article 58 (2) (d) of the Data Protection Regulation, the IMY requires MedHelp to

no later than two months after the decision becomes final, take the following measures.

1) Inform healthcare seekers who call 1177 about MedHelp's treatment of

personal data in accordance with Article 13 of the Data Protection Ordinance and Chapter 8. 6 § PDL.

2) Regarding audio files with recorded calls to 1177, which are answered by MedHelps

nurses within MedHelp's telephony platform, perform backup with

a set periodicity and keep the backups securely well separated from

the original information according to ch. § 12 HSLF-FS 2016: 40 and decide on how long

the backup copies should be saved and how often re-read tests of the copies should be done

according to ch. 3 13 § HSLF-FS 2016: 40.

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 MedHelp and carried out an inspection at MedHelp on the 20th

March 2019 to check how MedHelp processed personal data within the framework of

1177

IMY also initiated supervision of Voice Integrate Nordic AB (Voice) and Inera AB. The

It emerged that three regions used MedHelp as a care provider when seeking care

calls 1177 for healthcare advice and partly Inera AB to connect the calls to

MedHelp. IMY therefore initiated supervision against the Health and Medical Care Region

Stockholm, the Regional Board Region Sörmland and the Regional Board Region Värmland.

Justification of the decision

Legal background

National rules on health care

The tasks of the health care system are regulated in, among other things, the Health Care Act

(2017: 30), HSL.

Measures to medically prevent, investigate and treat diseases and injuries

defined as health and medical care, ch. 1 § HSL. By principal is meant that region

or the municipality which according to the law is responsible for offering health and medical care to

the population of the region or municipality. Within a principal's geographical area can

one or more care providers conduct business, ch. 2 § HSL. By caregiver is meant

government agency, region, municipality, other legal entity or sole trader

which conducts health and medical care activities, ch. 2 § 3 HSL. Regions and

municipalities may, while retaining leadership, conclude an agreement with someone else to

perform the tasks for which the county council or municipality is responsible, ch. 15 1 § HSL.

Anyone who has a constitutionally regulated responsibility for the provision of care is referred to as the principal.

The responsibility does not imply an obligation to run the business yourself, but the operation can

lie on someone else who is then referred to as a care provider (Bill 1981/82: 97 p. 33 f.). The

public responsibility as a principal does not imply a decision-making right over the care provider's

daily activities and it does not deprive the caregiver of the responsibility that comes with it

the role of caregiver (Bill 2016/17: 43 p. 86).

Anyone who belongs to or has belonged to the health care staff within the individual

According to ch. 6, the health service may Sections 12–15 of the Patient Safety Act (2010: 659),

(PSL) does not unauthorizedly disclose what he or she in his or her business has learned about one

individual health condition or other personal circumstances. For the general public

activities apply to the Public Access to Information and Secrecy Act (2009: 400) OSL.

Personal data responsibility and personal data assistant

According to Article 4 (7) of the Data Protection Regulation, a data controller means a
natural or legal person, public authority, institution or other body such as
alone or together with others determines the purposes and means of
the processing of personal data. About the purposes and means of treatment
determined by Union or national law of the Member States, it may
personal data controller or the specific criteria for how he or she is to be appointed
provided for in Union law or in the national law of the Member States.
According to ch. § 6 PDL is a care provider responsible for the processing of
personal data that the care provider performs in connection with individual-oriented care in its
activities, for example with regard to the obligation to keep a patient record.
According to Article 24 of the Data Protection Regulation, the controller shall include:
taking into account the nature, scope, context and purpose of the treatment, and
risks, implement appropriate technical and organizational measures to ensure
- and be able to show - that the processing is carried out in accordance with the Data Protection Regulation.
According to Article 4 (8) of the Data Protection Regulation, a personal data assistant refers to a physical
or legal person, public authority, institution or other body dealing with
personal data on behalf of the data controller. The personal data assistant receives
according to Article 29 of the Data Protection Regulation only process personal data on it
instruction of the data controller.
Basic principles and legal basis
Pursuant to Article 5 (1) (a) of the Data Protection Regulation, personal data shall be processed in one
legal, correct and transparent in relation to the data subject (principle of legality,
accuracy and transparency). According to Article 5 (1) (f), personal data must be processed in one way
ensuring adequate security of personal data, including protection against
unauthorized or unauthorized treatment and against loss, destruction or damage by
accident, using appropriate technical or organizational measures

(principle of integrity and confidentiality). According to the article, personal data controllers must

5.2 be responsible for and be able to demonstrate compliance with the principles of Article 5 (1) (the principle of

liability).

In order for a processing of personal data to be legal, it is required that it has the support of someone

of the legal bases set out in Article 6 (1) of the Data Protection Regulation. At

treatment for health care purposes, it is mainly Article 6 (1) (c) (legal

obligation) or 6.1.e (public interest or exercise of authority) which may be

applicable. According to Article 6 (3), the basis for the treatment referred to in Article 6 (1) (c)

and (e) is determined in accordance with Union law or the national law of a Member State which:

the person responsible for personal data is covered by. This means that if a caregiver

processing of personal data is necessary in order to fulfill a legal obligation or

perform a task of general interest so required for the processing to be legal that

the legal obligation or task of general interest is governed by national law

(or in Union law).

For activities according to, among other things, HSL, there are supplements

data protection provisions mainly in PDL and in HSLF-FS 2016: 40, as among others

contains rules on information security and on the physical protection of information systems.

According to ch. Section 2 of the PDL shall be information handling within health care

organized so that it meets patient safety and good quality and promotes

cost-effectiveness. Personal data must be designed and otherwise processed so that

the privacy of patients and other data subjects is respected. Documented

personal data must be handled and stored so that unauthorized persons do not have access to them.

Health information constitutes so-called sensitive personal data. It is forbidden to

process such personal data in accordance with Article 9 (1) of the Data Protection Regulation, unless

the treatment is not covered by any of the exceptions in Article 9 (2).

Registered right to information

Obligation of personal data controllers to voluntarily provide data subjects

information on the processing of personal data is provided in Articles 13 and 14 i

the Data Protection Regulation. It is relatively comprehensive information that should

provided to the data subjects. In addition to what is stated in Articles 13 and 14, it shall

care provider who is responsible for personal data according to ch. § 6 PDL leave further

information according to ch. 8 § 6 PDL to the registered. The information according to ch. 8 § 6

PDL shall include, among other things, what applies in terms of search terms, direct access and

disclosure of data on a medium for automated processing.

Safety in connection with the treatment

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.

The National Board of Health and Welfare has in HSLF-FS 2016: 40 on the basis of section 3 of the Patient Data Ordinance (2008: 360) and after consultation with IMY issued regulations needed for the enforcement of PDL in terms of security measures in full or in part automated processing of personal data. A caregiver responsible for personal data shall according to ch. § 12 HSLF-FS 2016: 40 ensure that personal data such as processed in information systems is backed up with a fixed periodicity and that the backups are stored securely, well separated from the original information.

The regulations specify in ch. § 12 thus a precautionary measure to be taken by personal data controllers. According to ch. 3, the care provider must § 13 decide on how long the backup copies should be saved and how often re-read tests of the copies should be done.

MedHelp's personal data responsibility

Of MedHelp's report of a personal data incident on 20 February 2019 (IMY: s case PUI-2019-689) states that MedHelp claims to be responsible for personal data as regards the processing of sensitive personal data in the form of audio files that have exposed to the internet without any protection mechanisms.

In this supervisory matter, MedHelp states that the company is a care provider as defined in 1

Cape. § 3 PDL and thus person responsible for personal data according to ch. § 6 of the same law for those personal data that the company processes when individuals call 1177. The company states further that, as a complement to the journal entries, the conversations are saved by recorded and stored. These recordings are part of the care documentation. MedHelp considers itself responsible for the personal data stored on Voice's server MediCall's account. When the calls could no longer be stored with Voice, they were transferred to MedHelp's servers.

IMY shares MedHelp's view that MedHelp is the care provider responsible for personal data according to ch. 2 6 PDL and that MedHelp for the individual-oriented care that takes place in connection with the individual calling 1177 may process personal data for purposes relating to care documentation, for example by recording calls to 1177.

The responsibility for processing personal data about care seekers performed by MediCall

MedHelp's information in the supervisory matter

Regarding MediCall's role in healthcare counseling by telephone, MedHelp has among otherwise stated the following.

MedHelp has hired MediCall as a subcontractor for healthcare advice by telephone when individuals call 1177. MediCall is a Thai company with operations in Thailand. MedHelp receives approximately 3 million calls per year within the framework of 1177. 20 percent of the traffic goes to MediCall and the rest to MedHelp. All nurses have Swedish nurse identification and meets the requirements of the agreements with the regions.

The nurses who work for MediCall are employed by MediCall. Nurses at both MedHelp and MediCall for notes in MedHelp's journal system Princess and the telephone calls are recorded to 1177.

MedHelp is the responsible care provider. Caregivers and patients are in Sweden when care is provided. MediCall is required to keep records. To record the calls is used

balancing of interests as a legal basis.

Integrity Protection Authority

Registration number: DI-2019-3375

Date: 2021-06-07

7 (23)

On October 15, 2012, MedHelp entered into an agreement with MediCall regarding
health care counseling and in connection with this a personal data assistant agreement was concluded.
On October 1, 2016, the parties entered into a supplementary agreement and a new agreement entitled “Agreement
regarding health care counseling services by telephone ”. A supplementary agreement to this agreement
was drawn up and signed on 1–2 March 2019. Appendix 4 to the supplementary agreement can be found
also a new personal data assistant agreement that replaces the previous one
the personal data assistant agreement from 2012. MedHelp has stated that the agreement and
The personal data assistant agreement expires on 31 August 2019, including MediCalls
processing of personal data related to 1177 ceases.

MediCall's information in the incident report

After IMY asked questions to MediCall, MediCall on 19 June 2019 supplemented its
notification of the personal data incident and thereby stated, among other things, the following.
MediCall is a Thai company, which provides advice by phone and others
communication channels in accordance with MedHelp's standards and routines on behalf of
MedHelp. The business is conducted only in Thailand. The personal information is added
on-duty nurse via MedHelp's medical record system on a screen. The nurse
answers and sees information based on what the caller has keyed in. After the conversation
or a journal is kept during the call. When the call is completed, the journal is closed
and can not be reopened by the nurse. The call is stored in MedHelp's system directly.
MediCall then sees the journal in MedHelp's system, works in the system, and documents
in MedHelp's system, no information is saved by MediCall. The IT system is called Collab.

When the incident occurred, the calls came in via Biz, which handles incoming and outgoing call. The calls were recorded by Biz and stored by Voice on behalf of MedHelp. MediCall has in its agreement 2012-09-02 with MedHelp a clause that prescribes that the processing of personal data shall take place in accordance with applicable law. New personal data assistant agreements including agreements on confidentiality were signed on March 1, 2019. MediCall has listed Voice as a personal data assistant but is a little unsure about this issue then MediCall sees them as a supplier directly to MedHelp. Nothing a personal data assistant agreement between MediCall and Voice has been signed.

On August 29, 2019, MediCall on its own initiative submitted a document to IMY as supplement to their report of personal data incident. At the top of the document, which is dated October 30, 2012, states the Health and Medical Care Administration, Stockholm County Council, registration number HSN 0805-0652 and the subject “Regarding the request for subcontractor approval '. Under the heading “Describe how you ensure that the agreement is fulfilled with the help of the subcontractor regarding the points ”appears among other that MedHelp does this to improve staffing during on-call time, which will provide a higher availability of health care counseling by telephone to the Care Guide (point 3). IN paragraph 5 states that all services performed by MediCall will comply with MedHelps quality management system.

IMY's assessment

Swedish health care has extensive regulation. In addition to the provisions of The Data Protection Regulation is of central importance to HSL. The law contains provisions on how Swedish health and medical care activities are to be organized and conducted. Measures to medically prevent, investigate and treat diseases and injuries defined as health and medical care, ch. 1 § HSL. By principal is meant that region or the municipality which according to the law is responsible for offering health and medical care to the population of the region or municipality. Within a principal's geographical area can

one or more care providers conduct business, ch. 2 § HSL. By caregiver is meant

government agency, region, municipality, other legal entity or sole trader

which conducts health and medical care activities, ch. 2 § 3 HSL.

Regions and municipalities may, with retained leadership, conclude an agreement with someone

another to perform the tasks for which the county council or municipality is responsible, ch. 15

1 § HSL. Anyone who has a constitutionally regulated responsibility for the provision of care is designated

principal. The responsibility does not imply an obligation to run the business yourself, but

the operation may be on someone else who is then referred to as a care provider (Bill 1981/82: 97 p.

33 f.). The public responsibility as principal does not imply control over

the caregiver's daily activities and it does not deprive the caregiver of the responsibility either

accompanies the role as caregiver (Bill 2016/17: 43 p. 86).

MedHelp is the care provider responsible for personal data for the processing of personal data

which takes place in connection with the healthcare advice that MedHelp has been commissioned by

regions to perform. This means that MedHelp according to Article 5 (2) i

the Data Protection Regulation must be able to show that personal data is processed in such a way

compliance with the principles set out in Article 5 (1).

In order for a processing of personal data to be legal, it is required that it has the support of someone

of the legal bases set out in Article 6 (1) of the Data Protection Regulation. At

treatment for health care purposes, it is mainly Article 6 (1) (c) (legal

obligation) or 6.1.e (public interest or exercise of authority) which may be

applicable. According to Article 6 (3), the basis for the treatment referred to in Article 6 (1) (c)

and (e) is determined in accordance with Union law or the national law of a Member State which:

the person responsible for personal data is covered by. This means that if a caregiver processing of personal data is necessary in order to fulfill a legal obligation or perform a task of general interest so required for the processing to be legal that the legal obligation or task of general interest is governed by national law (or in Union law).

In health care, the Data Protection Ordinance is supplemented by the PDL, which contains provisions on, among other things, who is responsible for personal data, if the obligation to keep a medical record and of permitted purposes for the treatment of personal data. According to ch. Section 3 of the PDL covers the scope of activity of the PDL referred to in, among other things, the Health and Medical Services Act (2017: 30), HSL. The determination in 2 Cape. Section 6 PDL that the care provider is responsible for personal data is a national specification of Article 4 (7) of the Data Protection Regulation.

A healthcare provider needs to process health information and sometimes other special information as well categories of personal data according to Article 9 (1) of the Data Protection Regulation, so-called sensitive personal data. It is basically forbidden to treat sensitive personal data according to the same article. The exceptions to the ban are set out in Article 9.2. For healthcare, there is an exception in Article 9 (2) (h) that applies provided that there is a statutory duty of confidentiality in accordance with Article 9 (3).

For Swedish health care, it is mainly the regulation in HSL and PDL as well of the duty of confidentiality in OSL and in ch. 6 §§ 12-15 PSL which states the legal support for that the processing of personal data is lawful within the meaning of Article 6 (1) (e), (2) and 6.3 and 9.2 h and 9.3 in the Data Protection Ordinance (Bill 2017/18: 105 p. 58 and 94 and prop. 2017/18: 171 pp. 105).

Through both MedHelp's and MediCall's data, it has emerged that both MedHelp and MediCall have taken measures that fall under the concept of health and

healthcare according to the definition in ch. § 1 HSL as regards 1177 through its measures for to medically prevent, investigate and treat diseases and injuries. The relationship is regulated by agreements and personal data assistant agreements. MediCall has to be able to perform healthcare processed personal data. This has been done by MediCall personal data regarding care seekers on a computer screen via MedHelp's medical record system and by answering a call on 1177. MediCall has collected during the call personal data by entering care documentation in MedHelp's medical record system, which also involved the processing of personal data.

However, MediCall is a Thai company operating in Thailand. The means the Swedish regulations in the field of health care are not applicable, even if the nurses who work at MediCall have Swedish identification. MediCall has thus not been imposed national tasks and responsibilities through the provisions of HSL and is not a care provider under Swedish law. MediCall is covered therefore also not of the scope of application of PDL according to ch. § 3 PDL, where it is stated that PDL is applied in caregivers' processing of personal data in health and healthcare. This further means that MediCall cannot be required to keep records in accordance with 3 Cape. PDL, as MedHelp stated.

The duty of confidentiality for private care providers is regulated in Chapter 6. 12–15 §§ PSL. It is stated that main rule, that whoever belongs to or belonged to health care personnel within it individual health care may not unauthorizedly disclose what he or she in his or her business has got to know about an individual's health condition or other personal conditions. Of ch. Section 2 of the PSL states that health care refers to the PSL activities covered by HSL or other national regulations on health and

the health care area, such as the Dental Care Act, the Insurance Medical Insurance Act

investigations etc. MediCall's operations are not covered by the national ones

the provisions neither in HSL nor in any of the other specified statutes which

means that neither ch. PSL is applicable. MediCall therefore lacks one according to Swedish

properly regulated duty of confidentiality.

The provisions in ch. 6 PDL on cohesive record keeping and in ch. 25 11 § 3

OSL means that two or more Swedish care providers can initiate a voluntary collaboration in

care purpose by following the provisions in ch. 6 PDL (cf. prop. 2007/08: 126 p. 132 f

that the individual health care can seek guidance for assessments of

the duty of confidentiality in confidentiality provisions). If MediCall has been a Swedish healthcare provider -

i.e. covered by HSL, PSL and PDL - MedHelp and MediCall could have started one

voluntary co-operation for care purposes by following the provisions in Chapter 6. PDL om

coherent record keeping.

MedHelp is the care provider and the legal support for the treatment of those involved

personal data is a legal obligation or public interest within the meaning of Article 6 (1) (c) or (e)

the Data Protection Ordinance, which is laid down in Swedish law in statutes such as PDL and

HSL in accordance with Article 6 (3) of the Data Protection Regulation. Legal support to get

processing sensitive personal data despite the prohibition in Article 9 (1) is found in Article 9 (2) (h) and

9.3. Balance of interests under Article 6 (1) (f) of the Data Protection Regulation is in this

context does not provide an applicable legal basis.

By using MediCall as a subcontractor for healthcare advice, MedHelp has

by telephone when individuals call 1177 has provided health and medical care and has thereby sounded

MediCall processes personal data without legal support in Swedish law and without it

there is a statutory duty of confidentiality in the manner required by Article 9 (3) (i)

the Data Protection Regulation.

Integrity Protection Authority

On October 15, 2012, MedHelp entered into an agreement with MediCall regarding
"Healthcare advice" and in connection with this a personal data assistant agreement was concluded.
On October 1, 2016, the parties entered into a supplementary agreement and a new agreement entitled “Agreement
regarding health care counseling services by telephone ”. A supplementary agreement to this agreement
was drawn up and signed on 1–2 March 2019. Appendix 4 to the supplementary agreement can be found
also a new personal data assistant agreement that replaces the previous one
the personal data assistant agreement from 2012.
The fact that the Swedish rules regarding health care do not apply to one
Thai company can not be replaced by a personal data assistant agreement or any
other contract structure. By personal data assistant is meant a physical or legal
person, public authority, institution or other body dealing with
personal data on behalf of the controller, Article 4 (8) (i)
the Data Protection Regulation. MediCall provides care and cannot constitute one
personal data assistant in that context, when a care provider must have one
independent support for processing personal data, which MediCall lacks.
IMY states that MedHelp, as the care provider responsible for personal data according to ch. § 6
PDL, at least from 25 May 2018 to 31 August 2019 in connection with that
care seekers call 1177 for health care advice provided personal information partly on
computer screen, partly by phone to MediCall and let MediCall collect personal data for
MedHelp's care documentation despite the fact that MediCall is not covered by HSL and thus not
nor are they covered by the provisions of the PSL and the PDL. These treatments have been lacking
legal aid in Swedish law in the manner required under Article 6 (3) and performed without it
there is a statutory duty of confidentiality in the manner required by Article 9 (3) (i)

the Data Protection Regulation. The proceedings have thus lacked a legal basis according to the article 6 and carried out in violation of the prohibition on the processing of sensitive personal data in Article 9 (1) (i) the Data Protection Regulation. As a result, the treatment has also taken place in violation of the principle on the legality of Article 5 (1) (a) of 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.

On 21 February 2019, IMY received MediCall's report of a personal data incident (IMY case PUI-2019-698). The incident is described as “Infringement of subcontractors (Voice Integrate Nordic ab) server. ” The incident concerns patients. Personal data such as covered by the incident are stated to be health, social security number and identification information, such as first and last name. After IMY asked questions to MediCall MediCall stated on 19 June 2019, among other things, that the calls were stored at Voice on commissioned by MedHelp.

On 21 February 2019, IMY received Voice's report of a personal data incident (IMY's case PUI-2019-705). 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 concerns patients and business users to a lesser extent. Personal information covered by the incident are stated to be health, social security number, identifying information such as first and last name and contact information.

Information from Voice in the supervisory case DI-2019-2488

Voice has stated the following, among other things.

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 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.

Voice and MedHelp have entered into a "Delivery agreement - services" signed on 1 September 2012. According to the agreement, Voice and MedHelp have had a close relationship for many years cooperation in technology, security and possible improvements in both technology, services as well as production. The agreement describes services such as “Recording (within systems) CC-50, “Recording calls”, “Search functions for retrieval” and “Filtering or deleting of recordings according to the customer's wishes ”. The delivery agreement applies from 2012-09-01 Empty. 2019-06-30.

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, but that one call corresponds to

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

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

calls from people who called 1177 the healthcare information and then connected on

to MedHelp and MediCall.

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. It is true that data files with recorded calls

transferred from MedHelp to Voice NAS, a networked storage device.

This has been caused by Medhelp's own server having crashed. Helps

server problems started as early as 2013 and then escalated and led to an emergency

situation in the fall of 2015. Voice management did not participate in or enforce this decision, but

became aware that the files were there on February 18, 2019 when the incident

was noticed in the media.

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.

MedHelp's information in the supervisory matter

MedHelp has stated, among other things, the following in this 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. Voice had built one web application that allows you to listen to the audio files. MedHelp has used the call follow-up application. To be able to take part in recordings have MedHelp's staff had to be logged in to MedHelp's internal environment and beyond it also authenticate itself in the web application. For a reason unknown to MedHelp came the stored content is then posted online. Then the calls could not be stored with 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.

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. Point 11 states that MedHelp has the right to follow
reasonable notice and in an appropriate manner prepare himself and / or his representative opportunity
to inspect that the supplier's processing of personal data takes place in
compliance with the service agreement and that the supplier has taken appropriate
security measures to protect the personal data processed on behalf of
The MedHelp Group. Furthermore, it appears, among other things, that the party must be continuously under
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.

IMY's assessment

The audio files in the Voice NAS storage server at Voice contained recorded calls to 1177
as nurses at MediCall answered. As noted above, MedHelp is in
capacity of caregiver personal data controller for this personal data.

The personal data responsibility includes a responsibility for the personal data being processed in
in accordance with applicable data protection rules. It is clear from those, among other things
the basic principles of Article 5 and of Article 24. It covers, in accordance with Article 5 (2)
also that you should be able to show that you do it.

That MedHelp through an agreement has allowed MediCall and Voice to process the personal data
does not affect the scope of MedHelp's responsibilities. It is the person responsible for personal data
who has the ultimate responsibility for the correct and lawful treatment of
personal data. MedHelp is also responsible for security in connection with
the treatment.

As stated earlier, it is the question of personal data that has been documented in
in connection with healthcare advice when healthcare seekers called 1177 in the regions
Stockholm, Sörmland and Värmland. It is a question of a business like MedHelp
is a care provider and thus responsible for personal data. MedHelp must therefore in
in the capacity of personal data controller to take appropriate technical and organizational measures
measures to ensure a level of safety appropriate to the risk. At
the assessment of the appropriate level of safety, special consideration shall be given to the risks involved
the treatment entails, in particular from accidental or unlawful destruction, loss or
change or to unauthorized disclosure of or unauthorized access to the personal data that
transferred, stored or otherwise processed, Article 32 (1) and (2)
the Data Protection Regulation. Ensuring adequate security means that one must
adapt the level of safety to the risks of the treatment in question.
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
supervisory case DI-2019-2488 that as of 18 February 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 Articles 5.1 f and 32 of the Data Protection Ordinance and from ch. § 2 second
and the third paragraph PDL. There is also a special regulation in HSLF-FS 2016: 40 how
personal data about patients must be protected.
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. For private care providers, the duty of confidentiality is regulated in 6
Cape. §§ 12–15 PSL, which the health and medical care staff of a private care provider must
follow.
According to Article 32 (1) of the Data Protection Regulation, the controller shall take appropriate steps
technical and organizational measures to ensure a level of security that is
appropriate in relation to the risk of protection of the data being processed. According to the article
32.2, when assessing the appropriate level of safety, special consideration shall be given to those risks
which the treatment entails, in particular from accidental or unlawful destruction, loss
or change or to unauthorized disclosure of or unauthorized access to the personal data
transferred, stored or otherwise processed.
Integrity Protection Authority
Registration number: DI-2019-3375
Date: 2021-06-07
14 (23)
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.

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. MedHelp's responsibilities also include the storage of

personal information about care seekers that took place in Voice NAS.

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 when Voice took over

measures to prevent exposure to the Internet. 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 of unauthorized disclosure or unauthorized use

access to personal data.

MedHelp has stated that MedHelp did not know about the personal data in Voice NAS

become accessible without protection mechanisms, that the stored content came out online by

unknown reason for MedHelp and that MedHelp became aware of

the personal data incident by Inera AB's Deputy CEO. IMY states that MedHelp has acted

only after the incident by examining the Voice NAS, transfer the care documentation

to own servers and give Voice instructions on deleting the calls, which Voice did

on March 7, 2019.

Against this background, IMY states that MedHelp has lacked sufficient capacity to

continuously ensure the confidentiality, integrity, availability and resilience of

treatment systems and services. According to IMY, MedHelp also lacked 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 this is a matter of many personal data, which are both sensitive

and subject to confidentiality, and that they have been exposed to the internet without protection which

meant they were accessible to anyone who had an internet connection. MedHelp has

thus not protecting the personal data against unauthorized touching or unauthorized access

and thus has not complied with its obligation as a personal data controller 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.

In accordance with the basic security principle of Article 5 (1) (f) of the Data Protection Regulation

personal data shall be processed in a manner that ensures appropriate security for

personal data, including protection against unauthorized or unauthorized processing and against

loss, destruction or damage by accident, using appropriate

technical or organizational measures. That the personal data has been exposed to

Internet without protection against unauthorized disclosure or unauthorized access means, according to IMY, that

the lack of security has been of such a serious nature that it also constitutes an infringement

of Article 5 (1) (f) of the Data Protection Regulation.

The obligation to provide information to care seekers

On 25 June 2019, IMY received a printout from www.1177.se about 1177

medical advice on the phone. The website states that behind 1177 Vårdguiden

Swedish healthcare through all regions is in collaboration. 1177 is a national telephone number for medical advice that you can call around the clock. Each region runs its own business for health counseling either under its own auspices or through procured subcontractor. The calls that are counseling calls are recorded. The question "Who is responsible for the personal data being handled correctly?" answered as follows.

“It is your healthcare provider who is responsible for ensuring that the personal data is handled correctly and legally. When care is provided by a region, there are one or more boards in the region who are ultimately responsible. In private care, it is the company or it activities that carry out the care that is responsible. "

MedHelp stated, among other things, the following at the inspection on March 20, 2019. MedHelp receives approximately 3 million calls per year within the framework of 1177. What information about personal data processing to be provided and by whom is regulated in the agreement with the Health and Medical Care Administration, HSF (Region Stockholm, IMY's note), which is responsible for to inform those who call the health information 1177. A few weeks ago no information was provided, but now some information is provided. MedHelp has not available what information is given in the voicemail. MedHelp can not be purely practical provide information in the voicemail as it is HSF that controls it. MedHelp represents HSF and the trademark 1177, so MedHelp must not tell a person that he has come to MedHelp. MedHelp provides information on its website that MedHelp processes personal data. On April 25, 2019, MedHelp states that for Region Stockholm informs the caller that the call will be recorded in patient safety and quality purposes, that the agreement with the Stockholm Region constitutes one publicly procured agreement where the terms of the agreement have thus been drawn up by the region and that as a service provider to the region, it is not possible for MedHelp to decide which one information to data subjects to be provided.

IMY's assessment

The person responsible for personal data must, in accordance with Article 12 (1) of the Data Protection Regulation take appropriate measures to provide the data subject with all information in accordance with Articles 13 and 14 in a concise, clear, comprehensible and easily accessible form, with use of clear and unambiguous language, in particular for information that is specifically targeted to children. Article 13 sets out the information to be provided by the controller provide if the personal data is collected from the data subject.3 in accordance with Article 13 (1), the controller shall provide information on, inter alia: identity and contact details for the personal data controller, contact details for the Data Protection Officer, where applicable, the purposes of the processing for which the personal data are intended as well as the legal basis for the processing. The personal data controllers shall also, in accordance with Article 13 (1) (f), provide specific information on: he intends to transfer personal data to a third country.4

Article 14 of the Data Protection Regulation specifies the information to be provided by the controller personal data are not collected from the data subject.

4 Where applicable, information that the data controller intends to transfer personal data to a third country or an international organization and whether there is a decision by the Commission on an adequate level of protection; or missing or, in the case of the transfers referred to in Article 46, 47 or the second subparagraph of Article 49 (1), reference to appropriate or appropriate protection measures and how a copy of them can be obtained or where these have been made available.

The obligation to provide information is extensive and a basic precondition for individuals must gain knowledge of and control over how their personal data is processed.

Requirement of transparency is a fundamental principle under Article 5 (1) (a) (i)
the Data Protection Regulation. Recital 60 of the Data Protection Regulation states that the principles
if fair and transparent treatment requires the data subject to be informed that
treatment takes place and the purpose of it. The person responsible for personal data should go to it
registrants provide all additional information required to ensure a fair
and open processing, taking into account the specifics of personal data processing
circumstances and context.
According to Article 13 (2), information shall be provided, inter alia, that there is a right to:
by the personal data controller request access to personal data. A caregiver should
also follow ch. 8 § 6 PDL which states what information the care provider must provide
the data subject in addition to what is stated in Articles 13 and 14. That information
shall include, inter alia, what applies in terms of search terms, direct access and
disclosure of data on a medium for automated processing.
IMY states that the public responsibility for the Stockholm Region as principal according to
HSL does not imply any decision-making power over MedHelp's day-to-day operations and that
does not deprive MedHelp of the responsibility that comes with the role of caregiver and
personal data controller. Liability in Article 5 (2) of the Data Protection Regulation
means that MedHelp is responsible for and must be able to show that MedHelp
complies with the basic data protection principles set out in Article 5 (1). That's it
MedHelp, which has the ultimate responsibility for ensuring that the principle of openness is followed by
Care seekers receive the necessary information about the processing of personal data.
When a healthcare seeker calls 1177, MedHelp collects as the person responsible for personal data
caregivers enter personal data for purposes related to care documentation. IMY
notes that according to Article 13 of the Data Protection Regulation and Chapter 8 Section 6 of the PDL is set
extensive requirements for information that MedHelp does not provide. It is not enough that
MedHelp in a voicemail message informs care seekers that the call is coming

recorded for patient safety and quality purposes. For example, information is completely missing that MedHelp is responsible for personal data, about MedHelp's contact information, that personal data is collected for purposes related to healthcare documentation, if the legal the basis for the treatment and that there is a right to it personal data controllers request access to personal data. It also has completely there was no information that personal data had been transferred to third countries. Even that supplementary information required according to ch. 8 § 6 PDL is missing.

Because MedHelp does not inform care seekers in connection with the collection of personal data during telephone calls to 1177, in addition to a voicemail message that The call is recorded for patient safety and quality purposes, IMY states that MedHelp has processed personal data in breach of Article 13 and the specified requirement of information to registered persons that appears from ch. 6 § PDL.

Article 5 (1) (a) of the Data Protection Regulation states that personal data must be processed in a legal, correct and transparent manner in relation to the data subject. Absence of information under Article 13 is assessed, as it significantly restricts the care applicant's conditions to exercise their rights, be so extensive and so serious that the deficiency is deemed to be contrary to the principle of transparency in Article 5 (1) (a).

Responsibility for backup

MedHelp states, among other things, the following in the supervisory matter. The recording of calls to 1177 which is answered by MedHelp's nurses takes place within MedHelp's own telephony platform. The calls are recorded and then stored on a storage server. There is no backup of the audio files. MedHelp has a special solution that will last

many years without backup. The files are located on multiple disks in a RAID system. So have
the solution has always been in place for MedHelp's calls. Recorded calls can be played back by
staff in MedHelp's patient safety center. A hit list can be generated in the system
and by clicking on a line you can proceed to the journal entry and
play the call.

IMY's assessment

According to Article 32 (1) of the Data Protection Regulation, the controller is obliged to take
appropriate technical and organizational security measures. According to Article 32 (2), at
the assessment of the appropriate level of safety takes special account of the risks involved
the treatment entails, in particular from accidental or unlawful destruction, loss or
change or to unauthorized disclosure of or unauthorized access to the personal data that
transferred, stored or otherwise processed. Ability to restore
the availability and availability of personal data in a reasonable time at a physical or technical
incident is, in accordance with Article 32 (1) (c), a measure which may be appropriate to:
ensure a level of safety that is appropriate in relation to the risk.

MedHelp processes within its telephony platform personal data about care seekers in
audio files with recorded calls to 1177. This takes place in MedHelp's operations according to HSL for
purposes relating to healthcare documentation. The sensitive nature of personal data, that
the personal data is collected in a confidential context relating to healthcare advice,
the scope of the treatment and the high risks entail high demands on them
security measures to be taken by Medhelp in accordance with Article 32 (1) of the Data Protection Regulation.

HSLF-FS 2016: 40 contains explicit regulations on backup. One
According to ch. 3, care providers must § 12 HSLF-FS 2016: 40 ensure that personal data
which are processed in information systems are backed up with a fixed periodicity
and that the backups are stored securely, well separated from
the original information. The care provider must also decide on how long the backups will last

saved and how often re-reading tests of the copies are to be performed, Chapter 3, Section 13 HSLF-FS

2016: 40. The National Board of Health and Welfare's regulations constitute national law that complements and

specifies the Data Protection Regulation and makes an explicit requirement

backup. IMY states that backup is a security measure that

MedHelp shall take steps to comply with the requirements of Article 32 (1) of the Data Protection Regulation.

MedHelp's use of robust storage media, such as a RAID system, does not constitute backup. A RAID system does not offer

the protection that

means that the data can be recreated if an incident occurs that affects them

stored the accuracy of the data, for example if the system is affected by malware. To

MedHelp uses a RAID system, however, is important for MedHelp's ability

continuity of treatment, ie. to continuously ensure confidentiality, integrity,

availability and resilience of treatment systems and services in that way

as set out in Article 32 (1) (b) of the Data Protection Regulation.

Both measures taken to ensure continuity in daily operations, to

example by using a RAID system, as steps taken to be able to

return to normal operation after an incident, such as backup, are measures

to ensure availability. However, this does not mean that these measures can

replace each other, without complementing each other.

IMY states that MedHelp, by not backing up audio files with recorded

calls to 1177 within MedHelp's telephony platform, have processed personal data in violation

with Article 32.1.

In accordance with the basic security principle of Article 5 (1) (f) of the Data Protection Regulation

personal data shall be processed in a manner that ensures appropriate security for
personal data, including protection against unauthorized or unauthorized processing and against
loss, destruction or damage by accident, using appropriate
technical or organizational measures. Loss of care documentation can mean one
high risk for the freedoms and rights of care seekers. Failure to implement
backup is therefore considered to be of such a serious nature that the deficiency also means one
infringement of Article 5 (1) (f) 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, among other things, the IMY may impose on the data controller
to ensure that the processing takes place in accordance with the Regulation and, if necessary, on one
specifically and within a specific period.

Pursuant to Articles 58 (2) and 83 (2) of the Data Protection Regulation, the IMY has the power to:
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 above assessed that MedHelp has violated Articles 5.1 a and f, 6, 9, 13 and 32.1

in the Data Protection Regulation. Infringements of these Articles may, in accordance with Article 83 (4) and 83.5 give rise to administrative penalty fees.

In view of the fact that the infringements found have affected a very large number care seekers who have been referred to call 1177 for health care advice and have included shortcomings in the handling of sensitive personal data such as health data, it is not the issue of minor infringements.

There is thus no reason to compensate for any of these violations the penalty fee with a reprimand. MedHelp must therefore be imposed with administrative penalty fees.

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.

Infringements of Article 5 (1) (a) and (f), 6, 9 and 13 of the Data Protection Regulation are covered by the higher penalty fee under Article 83 (5). The penalty fee shall thus up to EUR 20 000 000 or, in the case of a company, up to four% of total global annual sales in the previous financial year, whichever is the later value that is highest for infringements related to these items. Violations of article 32.1 is covered by the lower penalty fee under Article 83 (4). The penalty fee shall thus up to EUR 10 000 000 or, in the case of a company, up to two percent of total global annual sales in the previous financial year, depending at the maximum value of the infringement relating to this Article.

The term "a company" includes all companies engaged in an economic activity, regardless of the legal status of the entity or the way in which it is financed.

Recital 150 of the Data Protection Regulation states, inter alia, that if administrative penalty fees are imposed on a company, a company should be considered a company in that sense referred to in Articles 101 and 102 of the TFEU.

This means that the assessment of what constitutes a company must be based on definitions of competition law. The rules for group liability in the EU competition law revolves around the concept of economic unity. A parent company and a subsidiary is considered part of the same economic entity when the parent company exercises a decisive influence over the subsidiary. The decisive influence (ie control) can be achieved either through ownership or through agreements.

MedHelp AB's annual report states that MedHelp AB is part of a group, there MedHelp AB is 95 percent owned by MedHelp Group OY (a Finnish limited liability company) and to 5 percent of Meddet AB.

IMY believes that the fact that MedHelp is 95 percent owned by MedHelp Group OY means that the group in question shall be considered to be such an economic unit as

referred to in competition law. According to the annual report for the group was

annual sales SEK 223,013,000 for the financial year 2019.5

5

Four percent of sales correspond to SEK 8,920,000 and two percent to SEK 4,460,000.

Integrity Protection Authority

Registration number: DI-2019-3375

Date: 2021-06-07

20 (23)

The maximum amount of the penalty fees for infringements covered by

Article 83 (5) of the Data Protection Regulation is thus EUR 20 million and for infringements

covered by Article 83 (4) EUR 10 million.

Penalty fee for each violation

IMY has identified four violations concerning MedHelp's personal data processing

as personal data controller.

MedHelp 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 breach of Article 5 (1) (f) and Article 32 (1) of the Data Protection Regulation.

MedHelp has processed personal data by disclosing sensitive personal data

to MediCall and allow MediCall to collect personal data in violation of Article 5 (1) (a), (6) and

9.1 of the Data Protection Regulation. MedHelp has not provided information to

care seeker who called 1177 in violation of Article 5 (1) (a) and Article 13 (i)

the Data Protection Regulation. Finally, MedHelp has not backed up

care documentation in the form of audio files containing recorded calls to 1177 as

answered by MedHelp's nurses within MedHelp's telephony platform in violation of

Article 5 (1) (f) and Article 32 (1) of the Data Protection Regulation.

IMY assesses that the four infringements do not constitute interconnected treatments

and that a penalty fee should therefore be imposed per infringement.

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.6 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 penalty fee for each violation is determined as follows.

a) Processing of personal data about care seekers performed by MediCall

MedHelp receives approximately 3 million calls per year within the framework of 1177, of which MediCall

answered at 20 percent. It is thus about 600,000 calls per year as MediCall

answered. It is aggravating that it is a question of a comprehensive treatment of

sensitive and privacy-sensitive personal data, that the personal data processing

performed by an organization that is not covered by the privacy protections

which applies in the Swedish health care, e.g. the regulation on professional secrecy,

that care applicants have not been aware that the processing of personal data has taken place in

Thailand and that care seekers have not been able to refrain from the current one

personal data processing.

In view of the seriousness of the infringements and the administrative penalty fee

shall be effective, proportionate and dissuasive, the IMY shall determine the administrative

the penalty fee of SEK 3 million for this violation.

b) Exposed audio files on the Voice NAS storage server

MedHelp 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

6

Compare with Articles 83 (4) and 83 (5) of the Data Protection Regulation.

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. The caller can not object to personal data

processed for purposes related to care documentation.

In view of the nature of the data and the high security requirements for

personal data about care seekers, it is an aggravating circumstance that MedHelp,

as a care provider and personal data controller, has lacked control over the security of

personal data. MedHelp did not know that the personal data in Voice NAS had become

reachable without protective mechanisms. The stored content came out online by unknown

reason for MedHelp. MedHelp became aware of the incident by Inera AB's Deputy CEO.

MedHelp only acted after the incident by investigating Voice NAS, transfer

the care documentation to own servers and inform Voice about deleting the calls.

It is serious that a large amount of health information has been accessible to anyone who has one

internet connection for an unknown period of time.

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 8 million for this violation.

c) Information for care seekers

MedHelp receives approximately 3 million calls per year within the framework of 1177. The regulations

if information means that MedHelp must voluntarily make people seeking care

aware of MedHelp's personal data processing and their rights in connection

with MedHelp's processing of personal data. It is a matter of a comprehensive

duty to provide information, which is the basis for individuals to be able to have knowledge of and

control over how their personal data is processed.

It is aggravating that the lack of information concerns a large number of care seekers and that it

information corresponding to the requirements of the Data Protection Regulation is completely missing and

PDL, except for a voicemail message that the call will be recorded in

patient safety and quality purposes. The fact that information is not provided

including that MedHelp is responsible for personal data, the purposes and the legal

the basis for the treatment and that care seekers can turn to MedHelp to exercise

their rights under the Data Protection Regulation means that the conditions for

healthcare seekers to exercise their rights are significantly restricted. MedHelp also has

transferred personal data about patients to MediCall, a Thai company. It is

aggravating that there was a complete lack of information on the transfer of personal data to

Thailand, which is a third country.

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 500,000 for this violation.

d) Backup

MedHelp receives approximately 3 million calls per year within the framework of 1177. Lack of

backup at MedHelp thus concerns a large number of healthcare applicants. It is a

aggravating circumstance that there is no backup at all

care documentation on a large number of care applicants. Loss of care documentation can

entail a high risk for the freedoms and rights of care seekers.

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 sanction fee to SEK 500,000 for the violation.

Summary

IMY has found that MedHelp must pay a total administrative penalty fee of

SEK 12,000,000 for the established violations, of which SEK 3,000,000 pertains

the violation at point a), SEK 8,000,000 refers to the violation at point b),

SEK 500,000 refers to the violation at point c) and SEK 500,000 refers to

the infringement at point (d).

Instructions

MedHelp has not informed healthcare seekers in accordance with the requirements of the Data Protection Ordinance and Chapter 8 6 § PDL. The lack of information about, among other things, who is

personal data controller and his contact details limit the care applicant's

opportunities to, for example, be able to exercise the right to request access to personal data

which MedHelp collects in connection with care seekers calling 1177. MedHelp has

not backed up audio files that constitute care documentation according to

the Data Protection Ordinance and ch. 12-13 §§ HSLF-FS 2016: 40.

MedHelp receives about 3 million calls a year within the framework of 1177. It is a large

number of care seekers in need of healthcare advice who are affected by the shortcomings of

information and backup.

MedHelp must therefore be ordered in accordance with Article 58 (2) (d) of the Data Protection Regulation to:

as soon as possible and no later than two months after the decision has become final

the processing takes place in accordance with the Data Protection Regulation and supplementary national law regarding information for healthcare seekers and backup.

MedHelp has stated that MedHelp will suffer further damage if any injunctions for information to data subjects and backup are in conflict with MedHelp's agreement with the Stockholm Region or with procurement law legislation.

As a care provider and personal data controller, MedHelp has the ultimate responsibility for a legal processing of personal data, which includes that care seekers receive information about the processing of personal data and that backup measures taken.

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

MedHelp's CEO via e-mail