The Privacy Protection Authority

control of data processing

about seeking care in connection with

call to 1177 – a report

Diary number:

DI-2021-5220

Date:

2021-06-07

Content

Voice's role and responsibilities..... 11

Mailing address:

Box 8114

104 20 Stockholm

Website:

www.imy.se

E-mail:

imy@imy.se

Phone:

08-657 61 00

Background

On February 18, 2019, it was noticed that a large amount of calls to the number 1177

made available on a web server when Computer Sweden published an article with

headline "2.7 million recorded calls to 1177 completely unprotected on the internet".1

The article described how recorded calls to the advice number could be accessed

1177 on a server without password protection or other security.

The reporting was followed by a number of notifications of personal data incidents

was made to the Privacy Protection Agency (IMY), formerly the Data Inspectorate.2

Personal data incidents – security incidents where personal data e.g. changed, gone

lost or in the wrong hands - must be reported by the person in charge of personal data

to IMY if the incident may pose a risk to people's freedoms and rights.

Reports of personal data incidents were received, among others from the companies Voice Integrate

Nordic AB (Voice),3 MedHelp AB (MedHelp)4 and MediCall Co Ltd (MediCall).5

The article and received reports of personal data incidents led to IMY

launched surveillance against six actors who could be linked to the incident or

healthcare advice via the telephone number 1177; Voice, MedHelp, Inera AB (Inera), as well as

the regions of Stockholm, Värmland and Sörmland. During IMY's review,

the regions Värmland and Sörmland have stopped using MedHelp as healthcare providers

to answer calls to 1177.

The purpose of these reviews was to check the actors' connection to

healthcare advice via the telephone number 1177, who was responsible for personal data or

personal data assistant and how they lived up to their respective obligations according to

the data protection regulation6 and national supplementary law in health and

the healthcare area regarding safety and individual care seekers' right to information.

This report describes these supervisory cases and the connection between the different ones

the roles and responsibilities of the businesses at a glance. For more detailed information available

the supervisory decisions on the IMY website.7

The report describes the conditions under IMY's review.

IMY did not initiate supervision against MediCall because MediCall is a Thai company with

operations in Thailand and without representatives within the EU.

https://computersweden.idg.se/2.2683/1.714787/inspelade-samtal-1177-vardguiden-oskyddade-internet

On 1 January 2021, the Swedish Data Protection Authority changed its name to the Privacy Protection Authority.

3 IMY's case PUI-2019-705.

4 IMY's case PUI-2019-689.

5 IMY's case PUI-2019-698.

6 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural

persons with

regarding the processing of personal data and on the free flow of such data and on the cancellation of

directive 95/46/EC (General Data Protection Regulation).

7 https://www.imy.se/om-oss/arbetssatt/tillsyn/tillsynsbeslut/

1

2

The Swedish Privacy Protection Authority

Diary number: DI-2021-5220

Date: 2021-06-07

3 (11)

Introduction

What is the 1177 Care guide?

1177 Vårdguiden is a healthcare service that is offered and operated jointly by everyone

Sweden's 21 regions. The service is a gathering place for information about care and health

and which can be accessed both via the web and telephone. The telephone number 1177 is a national number

telephone number for healthcare advice where you can call for advice and guidance

of nurses.8

1177 Vårdguiden is not an individual actor, but each region operates its own

activities for health care consultancy, either under own auspices or through

subcontractors. To maintain the same quality, the regions are part of "a national network

with a common way of working".9

On the 1177.se website, the visitor is informed that all calls are recorded and that

counseling calls are recorded. Furthermore, it is informed that it is the respective care provider

who is responsible for the processing of personal data in journals and that personal data

handled correctly and legally.

The incident – unprotected exposure of audio files from

phone calls to 1177

In the personal data reports, the incident was described as unauthorized access there

people outside the organization, who lacked authorization, accessed sensitive information

personal data, i.a. about patients' health. The reason was stated to be a security hole10

and intrusion11 in the Voice server, Voice NAS, which resulted in sensitive personal data i

form of audio files with calls to 1177 had been exposed to the internet without any

protection mechanisms.12

The purpose of the Voice NAS server was initially to manage and store Voice internal files. The

was passive and lacked login accounts as it was intended to be used for Voice

own purposes from within the own network.

The incident was due to the Voice NAS, through a misconfiguration, being accessible from outside

system via a software security hole that caused the server to allow

unencrypted communication. As a result, a large number of conversations became accessible without

password protection or other security for anyone with an internet connection. That which

required to access the call files was the IP address of the server.

As of February 18, 2019, there were approximately 2.7 million files on the server. A conversation

corresponds on average to about three to four files, but can be up to ten files. IMY has

estimated the number of stored calls to be between 650,000 and 900,000.

Voice shut down the Voice NAS storage server on February 18, 2019 so that it does not

longer was reachable via the internet. It has not been possible to determine when the misconfiguration

took place or for how long the files were exposed.

https://www.1177.se/Stockholm/om-1177-vardguiden/1177-vardguiden-pa-telefon/om-1177-vardguiden-pa-telefon/.

https://www.1177.se/Stockholm/om-1177-vardguiden/1177-vardguiden-pa-telefon/om-1177-vardguiden-pa-telefon/.

10 IMY's case PUI-2019-705.

11 IMY's case PUI-2019-698.

12 IMY's case PUI-2019-698.

Actors who were subject to supervision

In the notifications of personal data incidents received from the companies Voice and MedHelp stated they were responsible for personal data. In the notifications it was stated further, that the incident was of considerable seriousness, that it was due to the human factor the factor and that the companies became aware of the incident via information from article i Computer Sweden or Inera AB. Supervision was initiated against both companies.

Supervision was also initiated against Inera in the light of the article and the information on Inera website that Inera manages and develops the common systems for 1177 at telephone that the regions need in their operations.

Both MedHelp and Inera stated that they acted on behalf of the Stockholm regions, Värmland and Sörmland with which they had an agreement. Supervision was initiated against that background also against the three regions.

Roles and requirements for security

Generally about the responsibility relationship between personal data controller and assistant

Clear responsibilities are crucial for adequate data protection.

It is the person responsible for personal data who must make the report when there has been one personal data incident. The fact that several notifications were received by IMY indicates that they are unclear circumstances surrounding who was responsible for the processing of personal data the personal data in the audio files. The role of the personal data assistant when it comes to personal data incidents is to notify it without undue delay personal data controller about a personal data incident that has occurred.

The person responsible for personal data must take appropriate technical and organizational measures
security measures to prevent unauthorized disclosure of or unauthorized access to
tasks. As a personal data controller, you must also sign an agreement with it
personal data assistant you hire. But personal data processors also have an obligation
to take appropriate technical and organizational security measures to prevent
unauthorized disclosure of or unauthorized access to the data.
In addition, organizations that process personal data must have a basic
IT security, regardless of whether you handle sensitive healthcare data or not.
Even if the actual handling of personal data takes place with a personal data assistant
it is always the person responsible for personal data who is ultimately responsible for them
personal data handled. This applies, among other things, to the processing of
the personal data is legal, that the data subjects receive information about the processing of
the personal data and that appropriate security measures are taken.
In addition, a personal data processor has its own obligations to take appropriate and
sufficient security measures to protect the personal data handled on
assignment by the person in charge of personal data.

In the case of personal data worthy of protection or sensitive to integrity, it is special
important that there are capabilities, routines and technical solutions in place that ensure that
the information does not become accessible to those who should not have access to it. It applies to both
the person responsible for personal data and personal data assistants.
If several actors are involved, there must be no doubts, divided opinions or ambiguities
about who is the personal data controller, who is the personal data assistant, and which

responsibilities and what obligations each has. The ratio between
personal data controller and personal data assistant must according to Article 28 i
the data protection regulation is regulated in an agreement and the assistant may only process
personal data on the responsible's documented instructions.

Liability issues according to the data protection regulation and requirements for
security

The Data Protection Regulation was introduced on 25 May 2018 and is the primary legal one
the regulation when processing personal data. This also applies when treating
personal data in healthcare.

The basic principles for processing personal data are stated in Article 5 i
data protection regulation. A basic principle is the requirement for security according to article
5.1 f, which states that the personal data must be processed in a way that ensures
appropriate security for the personal data, including protection against unauthorized or unauthorized access
treatment and against loss, destruction or damage by accident, with
use of appropriate technical or organizational measures. It is clear from Article 5.2
the so-called the liability, i.e. that the personal data controller shall be responsible for
and be able to demonstrate that the basic principles in point 1 are complied with.

Article 24 deals with the responsibility of the personal data controller. Article 24.1 states that
the personal data controller is responsible for implementing appropriate technical and
organizational measures to ensure and be able to demonstrate that the processing is carried out in
in accordance with the data protection regulation. The measures must be implemented taking into account
the nature, scope, context and purpose of the processing and the risks, of
varying degree of probability and seriousness, for the freedoms and rights of natural persons.
The measures must be reviewed and updated if necessary.

Article 32 regulates security in connection with the processing and also states
responsibility of personal data controllers to take security measures to protect

the personal data. According to point 1, the personal data controller shall and

the personal data assistant, taking into account the latest developments,

the implementation costs and the nature, extent, context and

purpose and the risks, of varying degree of probability and seriousness, for physical

people's rights and freedoms take appropriate technical and organizational measures

to ensure a level of security that is appropriate in relation to the risk (…). According to

point 2, when assessing the appropriate level of security, particular consideration must be given to the risks

which the processing entails, in particular from accidental or illegal destruction.13

Personal data controller is the natural or legal person (e.g. limited liability company, foundation,

association or authority) that determines the purposes for which data is to be processed

Additional requirements that must be regulated in an agreement between the person in charge of personal data and assistant

appear in Article 28 i

the data protection regulation, especially article 28.3 points c) and e).

13

and how the treatment is to be carried out.14 According to the Patient Data Act, a healthcare provider is

personal data controller for the processing of personal data carried out by the healthcare provider,

for example, regarding the care documentation in the individual-oriented care. 15

Personal data processor is a natural or legal person, public authority, institution

or other body that processes personal data for the personal data controller

account.16 Personal data controllers shall only hire personal data assistants who provide

sufficient guarantees to implement appropriate technical and organizational measures

in such a way that the processing complies with the data protection regulation and ensures

that the data subject's rights are protected.17 Personal data assistants may, as mentioned

only act on the instructions of the personal data controller,18 but

the data protection regulation also requires assistants to check that

the processing of personal data meets the requirements set out in the regulation. 19

It is the actual circumstances of the individual case that determine who is who

personal data controller and personal data assistant.

Requirements for transparency and information about who is who

personal data controller

The persons whose personal data is processed, here care seekers who call 1177, have

according to the data protection regulation right to receive information about how their personal data

treated.

According to the data protection regulation, personal data must be processed in an open manner i

relationship with the registered.20

The regulation contains requirements for clear and unambiguous information.21 This refers, for example

identity and contact details of the personal data controller, the purposes for and the

the legal basis for the processing and contact details for the data protection officer i

applicable cases.22

The information must be provided by the personal data controller when the data is collected

or at a later time if the data is collected from any other source.23

The Patient Data Act contains additional requirements for information to be submitted

the care provider to the patients, for example about the confidentiality and security regulations

which applies.24

On the 1177.se website, care seekers are informed that it is the care provider who is responsible

so that the processing of one's personal data takes place in a legal and correct manner.

Personal data responsibility includes, among other things, a responsibility to ensure that you have one

legal support for processing the personal data and for taking the necessary measures

Article 4.7 of the Data Protection Regulation.

2 ch. § 6 and ch. 2 Section 4 first paragraph 1 and 2 of the Patient Data Act (2008:355).

16 Data Protection Regulation Article 4.8.

17 Data Protection Regulation article 28.1.

18 Data Protection Regulation article 28.3 a.

19 Data Protection Regulation article 28.3 c.

20 Data Protection Regulation Article 5.1 a.

21 Article 12 of the Data Protection Regulation.

22 Article 13 of the Data Protection Regulation.

23 Data protection regulation article 13.1 resp. 14.3.

24 ch. 8 Section 6 of the Patient Data Act.

15

security measures. The responsibility also includes processing personal data on a

open way in relation to the registered,25 i.a. by providing clear

information about who is responsible for personal data. 26

On 1177.se, the information is given that if the region is a care provider, it is "one or more

boards or committees in the region that are ultimately responsible" and "within the private

care is the company or the business that provides the care that is responsible".

Incoming calls to 1177 are connected via a switchboard to a care provider who answers

the call from the care seeker. It may be the region that conducts the health and

the health care under its own auspices or a care provider that the region hires. During the review

information was missing for people who called 1177 from the Stockholm regions,

Värmland and Sörmland, among other things, about who was the care provider according to

the Patient Data Act and thus personal data controller.

The roles and responsibilities of the subjects of supervision and

the relationship between them

Overview description of the information flow

Calls to 1177 are initially routed to Inera, which provides the regions switchboard to

forward calls. At Inera, the so-called municipality ID, i.e. which municipality

calls are coming from to know which care provider the call should be routed to. The regions

Stockholm, Sörmland and Värmland27 had engaged MedHelp at the time of the incident

as healthcare providers, which is why Inera connected calls from these municipalities to MedHelp.

MedHelp had in turn hired MediCall as a personal data assistant and subcontractor

for healthcare advice via 1177 by phone. MediCall is a Thai company with

operations in Thailand, whose staff nurses answered calls from

care seekers during on-call hours.

Voice had developed the Biz software for audio recording and connection of calls from

MedHelp to MediCall. Voice also had the Voice NAS server.

Calls answered by MediCall were transferred to Voice NAS for storage. From

the Voice NAS server has the calls since due to a security flaw in connection with

a misconfiguration have been exposed to the Internet. MedHelp brought after that shortage

discovered over the care documentation to own servers and Voice deleted the calls on

MedHelp's instruction on March 7, 2019.

Data Protection Regulation Article 5.1 a.

Data Protection Regulation Article 13.1 a.

27 The regions of Sörmland and Värmland switched to conducting healthcare counseling via 1177 under their own auspices

during the end

of 2019.

25

26

Fig. 1, conversation and information flow between the actors.

The roles and responsibilities of the regions

The regions of Sörmland, Värmland and Stockholm are principally responsible for health care28 in their respective regions. Principals can contract with care providers, who

can be e.g. authorities, municipalities or companies, about carrying out the health and

healthcare for which the principals are responsible.29 The relevant regions have been included

personal data assistant agreement with Inera to have incoming calls forwarded to

1177 to be answered by MedHelp, which has been hired as a healthcare provider.

The relevant regions are responsible for personal data for the processing that takes place when they

collects information about telephone numbers and municipality IDs when individuals call 1177 so that

the calls can be answered by MedHelp. The regions are thus responsible for providing information

about that personal data processing.

The regions of Sörmland and Värmland

During the review, the regions Sörmland and Värmland30 have stopped hiring

MedHelp as a healthcare provider to answer calls to 1177.

The Swedish Privacy Protection Agency (IMY) found that the regions had not informed

care seeker about their treatment telephone number and information about which municipality

the person called from.

The IMY found that the lack of information contravened the principle of transparency i

the data protection regulation's article 5.1 a and against article 13 on the information that must

provided if personal data is collected from the data subject.

2 ch. Section 2 of the Health and Medical Care Act.

15 ch. Section 1 of the Health and Medical Care Act.

30 The regional board in each region is responsible for personal data.

28

29

IMY decided against that background, that the regions would pay an administrative

penalty fee of SEK 250,000 each.

Region Stockholm

In addition to processing information about callers' telephone numbers and municipality ID, in order to be able to direct calls to

the right healthcare provider, Region Stockholm31 also collected

enter personal information from MedHelp. The collection concerned call information from call to

1177 in the region and included i.a. social security number, contact reason, codes for symptoms,

referral (to e.g. self-care, närkut or care centre), business ID for

the care unit where the patient may have had an appointment, serial number of

journal entry (if one has been prepared) and time of call. The collection of

the call information from MedHelp concerned an extensive amount of sensitive

personal data concerning a large number of registered users.

Region Stockholm pseudonymises the data and uses the information to

develop the function of healthcare advice.

IMY stated that the Health and Medical Board when processing personal data

to direct calls to 1177 to the care provider MedHelp had not informed
care seekers about their treatment of telephone number and municipality ID. Health and
the medical board also did not inform about the collection from MedHelp by
personal data on care seekers who called 1177.
The IMY found that the lack of information contravened the principle of transparency in Article 5(1)(a),
as well as against articles 13 and 14 of the data protection regulation regarding the information that must
given to care seekers.
IMY decided against this background that the Health and Medical Board should pay a
administrative sanction fee of SEK 500,000.
IMY also presented according to article 58.2 d of the data protection regulation Health and
the health care board that, as soon as possible and no later than two months after the decision has been won
legal force, in accordance with articles 13 and 14 of the data protection regulation inform
care seekers who call 1177 about collection of telephone numbers and municipality ID for
the purpose of ensuring that calls to 1177 are taken care of by the healthcare provider MedHelp AB as well as
on the collection of call information from MedHelp AB for follow-up and
quality purposes.
Inera's role and responsibilities
Inera manages and develops the common systems for 1177 and the thereby
coherent healthcare advice on the phone that the regions needed in their
operations.32 Inera assisted, as personal data assistant, the regions with handling of
incoming calls by connecting them to MedHelp. Inera did not record
these conversations. IMY closed the supervision of Inera without action.
MedHelp's role and responsibilities
The regions of Stockholm, Sörmland and Värmland hired MedHelp as a healthcare provider for
to answer the care seeker's call to 1177. Calls were connected by Inera to MedHelp

32

The Swedish Health and Welfare Board is responsible for personal data in the Stockholm region.

www.inera.se/tjanster/1177-vardguiden-pa-telefon.

who took over the call. MedHelp conducted approximately three million counseling calls

per year via 1177.

As a healthcare provider and personal data controller, MedHelp processed personal data when

individuals called 1177. The processing of personal data took place by recording of

phone calls and care documentation in a record system.

MedHelp hired MediCall as personal data assistant and subcontractor for

healthcare advice via telephone when individuals called 1177 during on-call hours. Of the three

million calls per year that MedHelp received were handled approximately 20 percent at

MediCall.

MedHelp hired MediCall to improve on-call staffing. Then the business

was conducted in Thailand, one could take advantage of the time difference to offer a higher

availability of healthcare advice on 1177. MediCall's nurses brought

notes in MedHelp's journal system when calls were answered.

As the person responsible for personal data, MedHelp has an obligation to comply

the data protection regulation and national law for the processing of personal data within

health care.33 The responsibility includes fulfilling the obligations in

the data protection regulation, including the obligation to process personal data in an open manner

way in relation to the registered,34 i.a. by providing clear information

about the treatment and that MedHelp is responsible for personal data. 35

IMY stated that MedHelp in its capacity as healthcare provider and personal data controller had processed personal data in violation of the data protection regulation, the patient data act and the National Board of Health and Welfare's regulations and general advice on record keeping and treatment of personal data in healthcare (HSLF-FS 2016:40) in the following respects:

- personal data in audio files with recorded phone calls to 1177 had been exposed against the Internet without protection in the Voice NAS storage server. MedHelp thereby had i attribute of care provider and personal data controller failed to take appropriate technical and organizational measures to ensure a level of security that was suitable to prevent unauthorized disclosure of the personal data or unauthorized access to the personal data.
- MedHelp had no legal support in Swedish healthcare legislation and i the data protection regulation allowed the Thai company MediCall, which was not covered of the Health and Medical Care Act and regulations on confidentiality, providing care and process personal data about care seekers who called 1177. In support of that personal data processing, MedHelp established a personal data assistant agreement with MediCall, but such an agreement cannot replace the lack of legal support.
- MedHelp did not, apart from a voicemail message that the call was being recorded patient safety and quality purposes, informed care seeker who called 1177 about their personal data processing.
- MedHelp had not backed up calls to 1177 that MedHelp answered and recorded in its IT environment.

Data protection regulation article 5.1 f.

Data Protection Regulation Article 5.1 a.

35 Data Protection Regulation Article 12.1.

The IMY decided that MedHelp should pay an administrative penalty fee of 12
million kroner, of which kroner eight million referred to exposed sound files with recorded ones
phone calls to 1177 against the internet without protection, three million kroner meant that MedHelp
carried out personal data processing by hiring MediCall, five hundred thousand kroner
intended that MedHelp did not provide necessary information to care seekers who called
1177 and five hundred thousand kroner meant that MedHelp had not backed up
audio files in their IT environment.

The decision also included two injunctions. One concerned information for care seekers
whose calls to 1177 are answered by MedHelp.

The second order required MedHelp to carry out backup and
store the backup copies in a safe manner well separated from the original data,36 as well as
to decide how long the backups should be kept and how often
read-back tests of the copies shall be done.37

Voice's role and responsibility

Voice had developed the Biz software for audio recording and connection of calls from
MedHelp to MediCall. Voice also had the Voice NAS server.

Voice is a development company that produces software. Voice and MedHelp had
according to a delivery agreement entered into in 2012, a collaboration around technology, security and
improvements in services and production. The companies included one
personal data assistant agreement in May 2018. The agreements show that the assignment to Voice
included i.a. healthcare advice and recording of calls. Voice delivered calls
to MediCall through its switches through the Biz software, and also provided others

features, programs and support.

Recorded audio files with calls to 1177 were in the storage server Voice NAS when

the incident occurred.

IMY found that personal data in audio files with recorded phone calls to 1177

had been exposed to the Internet without protection in the Voice NAS storage server. Voice had

thereby, in the capacity of personal data assistant to MedHelp, failed to take appropriate measures

technical and organizational measures to ensure a level of security that was

suitable to prevent unauthorized disclosure of the personal data or unauthorized access

to the personal data.

The IMY decided that Voice should pay an administrative penalty fee of 650,000

crowns.

36

37

According to ch. 3 Section 12 HSLF-FS 2016:40.

According to ch. 3 Section 13 HSLF-FS 2016:40.