The Privacy Protection Authority's control of data processing about care seekers in connection with calls to 1177 - a report

Record number:

DI-2021-5220

Date:

2021-06-07

Content

Voice's role and responsibilities 11

Postal 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 number of calls to the number 1177

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

entitled "2.7 million recorded calls to 1177 completely unprotected on the Internet" .1

The article described how you could take part in recorded calls to the counseling number

1177 on a server without password protection or other security.

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

was made to the Privacy Protection Authority (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 responsible for personal data

to the IMY if the incident could pose a risk to human freedoms and rights.

Reports of personal data incidents were received, among other things. 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

initiated supervision of six actors that could be linked to the incident or

medical advice via telephone number 1177; Voice, MedHelp, Inera AB (Inera), and

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

the regions Värmland and Sörmland have ceased to use MedHelp as a care provider

to answer calls to 1177.

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

health care advice via telephone number 1177, who was responsible for personal data or

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

the Data Protection Regulation6 and national supplementary law in the field of health

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

This report describes these supervisory matters and the connection between the various

the roles and responsibilities of the activities in general. For more detailed information, see

supervisory decisions on the IMY website.7

The report presents the conditions during the IMY's review.

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

activities in Thailand and without EU representatives.

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

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

3 IMY case PUI-2019-705.

4 IMY case PUI-2019-689.

5 IMY case PUI-2019-698.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to

concerning the processing of personal data and on the free movement of such data and on the repeal of

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

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

1

2

Integrity Protection Authority

Registration 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 run 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

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

of nurses.8

1177 The care guide is not an individual actor, but each region conducts its own

activities for health care counseling, either in-house or through

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

with a common approach ”.9

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

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

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

handled correctly and legally.

The incident - unprotected exposure of audio files from

phone call to 1177

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

people outside the organization, who lacked authority, took part in sensitive

personal data i.a. on patients' health. The cause was stated to be a security hole10

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

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

protective 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 Voice NAS, through a misconfiguration, could be accessed outside

the system through a security hole in the software that caused the server to allow

unencrypted communication. As a result, a large amount of calls 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 to an average of 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 error configuration

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 case PUI-2019-705.

11 IMY Case PUI-2019-698.

12 IMY Case PUI-2019-698.

Actors covered by supervision

In the reports of personal data incidents received from the companies Voice and
With MedHelp, they stated that they were responsible for personal data. The notifications were stated
further that the incident was of significant seriousness, that it was due to the human
factor and that the companies became aware of the incident via information from the article in
Computer Sweden or Inera AB. Supervision was initiated against both companies.
Supervision was also initiated against Inera in the light of the article and information on Inera
website that Inera manages and develops the common systems for 1177 on
telephone that the regions need in their activities.
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 security requirements

In general about the relationship of responsibility between
personal data controller and assistant

Clear responsibilities are crucial for adequate data protection.
It is the person who is responsible for personal data who must report when one has occurred
personal data incident. The fact that several reports were received by the IMY indicates unclear
conditions regarding who was responsible for personal data for the processing of
the personal data in the audio files. The role of the personal data assistant in
personal data incidents is to notify it without undue delay
personal data controller in the event of a personal data incident.

The person responsible for personal data must take appropriate technical and organizational steps

security measures to prevent unauthorized disclosure or unauthorized access to

tasks. As a person responsible for personal data, you must also sign an agreement with it

personal data assistant you hire. But personal data assistants 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, whether or not you handle sensitive healthcare tasks.

Even if the actual handling of personal data takes place with a personal data assistant is

it is always the person who is responsible for personal data who is ultimately responsible for them

personal data handled. This applies, among other things, to the treatment of

personal data is legal, that the data subjects receive information about the processing of

personal data and that appropriate security measures are taken.

In addition, a personal data assistant has its own obligations to take appropriate and

adequate security measures to protect the personal data processed on

assignment by the person responsible for personal data.

Integrity Protection Authority

Registration number: DI-2021-5220

Date: 2021-06-07

When it comes to personal data that is worthy of protection or privacy, it is special

It is important that there are capabilities, routines and technical solutions in place that ensure that

the data will not be accessible to those who should not have access to it. This applies to both

the person who is responsible for personal data and personal data assistants.

If several actors are involved, there must be no doubt, divided opinions or ambiguities

about who is responsible for personal data, who is a personal data assistant, and which

responsibilities and what obligations each has. The ratio between

personal data controller and personal data assistant shall, in accordance with Article 28 i

the data protection regulation is regulated in an agreement and the assistant may only process

personal data on the person's documented instructions.

Liability issues according to the Data Protection Ordinance and requirements for

security

The Data Protection Ordinance was introduced on 25 May 2018 and is the primary legal one

the regulation in the processing of personal data. This also applies to the treatment of

personal data in health care.

The basic principles for the processing of personal data are set out in Article 5 (i)

the Data Protection Regulation. A basic principle is the requirement for security according to the article

5.1 f, which states that personal data shall be processed in a manner that ensures

appropriate security for personal data, including protection against unauthorized or unauthorized use

treatment and against loss, destruction or damage by accident, with

use of appropriate technical or organizational measures. Article 5 (2) states

the s.k. liability, ie. that the person responsible for personal data shall be responsible for

and be able to demonstrate compliance with the basic principles set out in paragraph 1.

Article 24 deals with the responsibility of the 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 treatment is carried out in

in accordance with the Data Protection Regulation. The measures shall be implemented taking into account

the nature, scope, context and purpose of the treatment and the risks, of

varying degrees of probability and seriousness, for the freedoms and rights of natural persons.

The measures must be reviewed and updated as necessary.

Article 32 regulates the security in connection with the processing and also states

the responsibility of the personal data assistant to take security measures to protect

personal data. According to paragraph 1, the controller and

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

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

purposes and the risks, of varying probability and severity, of physical

rights and freedoms of individuals take appropriate technical and organizational measures

to ensure a level of safety appropriate to the risk (…). According to

paragraph 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.13

The person responsible for personal data is the natural or legal person (eg limited liability company, foundation,

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

Additional requirements to be regulated in an agreement between the data controller and the assistant are set out in Article 28

of

the Data Protection Regulation, and in particular Article 28 (3) (c) and (e) thereof.

13

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

personal data controller for the processing of personal data performed by the care provider,

for example with regard to the care documentation in the individual-oriented care.15

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

or another body that processes personal data for the data controller

invoice.16 The person responsible for personal data shall only hire personal data assistants who provide

adequate 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 As mentioned, personal data assistants may

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

The Data Protection Regulation also requires assistants to check that

the processing of personal data meets the requirements of the Regulation.19

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

personal data manager and personal data assistant respectively.

Demands for openness and information about who is

personal data controller

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

according to the Data Protection Regulation the right to receive information about how their personal data

treated.

According to the Data Protection Ordinance, personal data must be processed in a transparent manner in

relation to the data subject.20

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

identity and contact details of the person responsible for personal data, the purposes for and the

the legal basis of the processing and contact details of the data protection officer in

where applicable.22

The information must be provided by the person responsible for personal data when the data is collected

or at a later date if the data is collected from another source.23

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

the caregiver to the patients, for example about the confidentiality and safety regulations

which applies.24

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

for the processing of one's personal data to take place in a legal and correct manner.

The responsibility for personal data includes a responsibility to ensure that you have one

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

Article 4 (7) of the Data Protection Regulation.

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

16 Article 4 (8) of the Data Protection Regulation.

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 8 chap. Section 6 of the Patient Data Act.

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

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

information about who is responsible for personal data.26

At 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” in the private sector

care is the company or business that conducts 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 hired by the region. During the review

there was a lack of information 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 the person responsible for personal data.

The roles and responsibilities of the supervised entities and

the relationship between them

General description of the information flow

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

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

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

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

as a care provider, which is why Inera linked calls from these municipalities to MedHelp.

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

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

operations in Thailand, whose employed nurses answered calls from

care seekers during on-call time.

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 then has the calls due to a security flaw associated with

an incorrect configuration has been exposed to the internet. MedHelp led after the shortage

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

MedHelp's instruction on March 7, 2019.

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

Article 13 (1) (a) of the Data Protection Regulation.

27 The regions Sörmland and Värmland switched to conducting health care counseling via 1177 under their own auspices at

the end

of 2019.

25

26

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

The roles and responsibilities of the regions

The regions Sörmland, Värmland and Stockholm are principals with responsibility for health and medical care28 in their respective regions. Principals can agree with caregivers, who

can be e.g. authorities, municipalities or companies, to carry out the health and

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

personal data assistant agreement with Inera to allow incoming calls to be diverted to

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

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

collects information about telephone numbers and municipal ID when individuals call 1177 so that

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

about the processing of personal data.

The regions Sörmland and Värmland

During the review, the regions Sörmland and Värmland30 ceased to engage

MedHelp as caregiver to answer calls to 1177.

The Privacy Protection Agency (IMY) found that the regions had not provided information

care seekers about their processing of telephone numbers and information about which municipality

the person called from.

IMY found that the lack of information was contrary to the principle of transparency in

Article 5 (1) (a) of the Data Protection Regulation and against Article 13 on the information to be provided

provided if personal data is collected from the data subject.

Chapter 2 Section 2 of the Health Care Act.

Chapter 15 Section 1 of the Health and Medical Services Act.

30 The Regional Board in each region is responsible for personal data.

28

29

Against this background, the IMY decided that the regions would pay an administrative fee

penalty fee of SEK 250,000 each.

Stockholm Region

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

the right care provider, Region Stockholm31 also collected

in personal data from MedHelp. The collection referred to call information from calls to

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

referral (to eg self-care, emergency department or health center), business ID for

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

journal entry (if established) and time of call. The collection of

the call information from MedHelp referred to an extensive amount of sensitive

personal data concerning a large number of data subjects.

Region Stockholm pseudonymizes the information and uses the information to

develop the function of health care counseling.

IMY stated that the Health and Medical Care Board in the processing of personal data

to direct calls to 1177 to the care provider MedHelp had not informed
care seekers about their processing of telephone numbers and municipality ID. Health and
The health care board also did not inform about the collection from MedHelp by
personal data about care seekers who called 1177.
The IMY found that the lack of information was contrary to the principle of transparency in Article 5 (1) (a),
and against Articles 13 and 14 of the Data Protection Regulation on the information to be provided
given to care seekers.
Against this background, the IMY decided that the Health and Medical Care Board would pay one
administrative sanction fee of SEK 500,000.
In accordance with Article 58 (2) (d) of the Data Protection Regulation, the IMY also presented
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
care seekers who call 1177 for collection of telephone numbers and municipality ID for
the purpose of ensuring that calls to 1177 are taken care of by the care provider MedHelp AB and
on the collection of call information from MedHelp AB for follow-up and
quality purposes.
Inera's role and responsibility
Inera manages and develops the common systems for 1177 and thus
coherent health care by telephone that the regions needed in their
activities.32 Inera, as a personal data assistant, assisted the regions with the management of
incoming calls by connecting them to MedHelp. Inera did not record
these conversations. IMY terminated the supervision of Inera without action.
MedHelp's role and responsibility
The regions of Stockholm, Sörmland and Värmland hired MedHelp as a care provider for
to answer the care applicant's calls to 1177. Calls were connected by Inera to MedHelp

32

The Health and Medical Care Board is responsible for personal data in the Stockholm region.

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

Integrity Protection Authority

Registration number: DI-2021-5220

Date: 2021-06-07

10 (11)

who took over the call. MedHelp conducted approximately three million counseling interviews per year via 1177.

As a care provider and personal data manager, MedHelp processed personal data when individuals called 1177. The processing of personal data took place by recording telephone calls and care documentation in a medical record system.

MedHelp hired MediCall as a personal data assistant and subcontractor for health care counseling by telephone when individuals called 1177 during on-call time. Of the three million calls per year that MedHelp received handled approximately 20 percent of MediCall.

MedHelp hired MediCall to improve staffing during on-call time. Then the business conducted in Thailand, one could take advantage of the time difference to offer a higher availability for health care counseling at 1177. MediCalls nurses led notes in MedHelp's medical record 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 a transparent manner way in relation to the registered, 34 i.a. by providing clear information about the processing and that MedHelp is responsible for personal data.35

IMY stated that MedHelp in its capacity as caregiver and personal data controller had processed personal data in violation of the Data Protection Ordinance, the Patient Data Act and the National Board of Health and Welfare's regulations and general guidelines on record keeping and treatment of personal data in health care (HSLF-FS 2016: 40) in the following respects:

- personal data in audio files with recorded telephone calls to 1177 had been exposed against internet without protection in the storage server Voice NAS. MedHelp then had in as a caregiver and personal data controller failed to take appropriate technical and organizational measures to ensure a level of security that was suitable for preventing the unauthorized disclosure of personal data or unauthorized use access to personal data.

MedHelp had without legal support in Swedish health care legislation and in data protection ordinance allowed the Thai company MediCall, which was not covered of the Health Care Act and provisions on professional secrecy, perform care and process personal data about care seekers who called 1177. In support of it personal data processing, MedHelp established a personal data assistant agreement with MediCall, but such an agreement can not replace the lack of legal support.

MedHelp did not have, in addition to a voicemail message that the call was recorded in patient safety and quality purposes, informed care seeker who called 1177 about their personal data processing.

- MedHelp had not backed up calls to 1177 which MedHelp answered and recorded in their IT environment.

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

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

35 Data Protection Regulation Article 12 (1).

IMY decided that MedHelp would pay an administrative penalty fee of 12
million kronor, of which eight million kronor referred to exposed audio files with recorded
phone call to 1177 against the internet without protection, SEK 3 million was intended for MedHelp
performed personal data processing by using MediCall, five hundred thousand kronor
intended that MedHelp had not provided the necessary information to the care applicant who called
1177 and five hundred thousand kronor 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 call to 1177 is answered by MedHelp.

The second injunction was for MedHelp to perform backup and
keep the backups securely separate from the original data, 36 and
to decide how long the backups should be saved and how often
re-reading tests of the copies shall be performed.37

Voice's role and responsibilities

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 develops software. Voice and MedHelp had
according to an agreement entered into in 2012, a collaboration on technology, security and
improvements in services and production. The companies included one
personal data assistant agreement in May 2018. The agreements state that the assignment to Voice
included i.a. health care counseling and call recording. Voice delivered calls
to MediCall via its switches through the Biz software, and also provided others

features, applications and support.

Recorded audio files with calls to 1177 were in the Voice NAS storage server 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, as a personal data assistant to MedHelp, failed to take appropriate technical and organizational measures to ensure a level of security that was suitable for preventing the unauthorized disclosure of personal data or unauthorized access to the personal data.

IMY decided that Voice would pay an administrative penalty fee of 650,000 kronor.

36

37

According to ch. 12 § HSLF-FS 2016: 40.

According to ch. 13 § HSLF-FS 2016: 40.