Decision

Diary no

2020-11-24

DI-2019-7782

Gnosjö municipality - Social Committee

Supervision according to the EU data protection regulation

2016/679 – camera surveillance at an LSS residence

Table of Contents

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Telephone: 08-657 61 00







## The Swedish Data Protection Authority's decision

The Data Inspectorate states that Gnosjö municipality - Social Committee under

period March 2019 - April 2020, a resident of an LSS residence1 was monitored by camera in his bedroom and thereby

processed personal data in violation of

- Article 5.1 a of the data protection regulation2 when the camera surveillance took place

without legal basis and legal support for the processing of

personal data i.e. not been legal. That the camera surveillance has been carried out

in a more intrusive way for the resident's personal privacy than what

which can be considered fair, reasonable and proportionate in relation to

the purpose, i.e. did not live up to the requirements for correctness and that

the camera surveillance took place without the resident's permission

information either according to the data protection regulation or

the camera surveillance act, i.e. did not live up to the requirements of transparency.

- Article 6.1 by processing personal data without having any

legal basis for it,

- Article 9.2 by processing sensitive personal data about

illness and health condition without having a legal support for it

the treatment,

- articles 35 and 36 by not having met the requirements of a

impact assessment and not have prior consultation with

The Swedish Data Protection Authority and

- Article 13 by not having fulfilled the requirement of information to it

registered (the resident) as well as

- Section 15 of the Camera Surveillance Act (2018:1200) by not having left

information about the camera surveillance through clear signage or on

some other effective way.

Administrative penalty fees

The Data Inspection Authority makes decisions with the support of articles 58.2 and 83 i

data protection regulation, ch. 6 Section 2 of the Act (2018:218) with supplementary

provisions to the EU's data protection regulation and § 25 point 4 i

The Camera Surveillance Act (2018:1200) that Gnosjö municipality - Social Committee for

1

Housing with special service according to the Act (1993:387) on support and service for certain people

handicapped.

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

on the protection of natural persons with regard to the processing of personal data and on that free flow of such data and on the repeal of Directive 95/46/EC (general data protection regulation).



the violations of Article 5(1)(a), Article 6(1), Article 9(2), Article 13, Article 35 and Article 36 of the Data Protection Ordinance and Section 15 of the Camera Surveillance Act shall pay an administrative sanction fee of SEK 200,000.

## Account of the supervisory matter

### Background

On 2 May 2019, the Data Protection Authority received a report from a relative of a resident of an LSS accommodation in Gnosjö municipality according to which the social committee i Gnosjö municipality (hereinafter the social committee) processes personal data through to camera monitor a resident in one of the municipality's LSS residences. According to notification, the social committee must have stated that the camera surveillance takes place with support of an approval/consent from the resident's family and former trustee to the resident. There is no approval/consent according to the submitter of the report.

The Swedish Data Protection Authority has due to the information contained in the notification initiated supervision with the aim of reviewing the processing of personal data which the social committee must have carried out through camera surveillance is in accordance with the data protection regulations and the camera surveillance law.

The supervisory case was initiated with a supervisory letter on 15 July 2019. Response to the supervisory letter was received on 21 August 2019. Supplementary letters from the social committee has received on 2 December 2019, 11 May 2020, 12

August 2020 and November 4, 2020.

What emerged in the case

The social welfare committee has processed personal data in real time

camera surveillance of a resident in an LSS residence in order to increase their security

accommodation. The camera was installed in March 2019 and surveillance ended on the 29th

April 2020 in connection with the business being taken over by another contractor.

The Social Committee has stated the following. The resident has lived in the LSS accommodation

since autumn 2013. She needs support in her everyday life around the clock from two people,

when she exposes herself to serious self-harming behavior and needs help to

prevent this. In emotionally difficult situations, he wants to be himself

bedroom with the door closed, the staff has then been in the living room and

be prepared to step in if necessary. It has happened that it has become completely quiet inside



with the resident and when staff opened the door to see how he was doing,

she slept but was awakened when the door was opened. The resident has then again become

emotionally upset and risk of self-injurious behavior has been present. At others

on occasions it has happened that the resident has seriously injured himself without

staff have heard something.

During the resident's first time at the LSS accommodation, there were periodically three members of staff

service, despite that it happened several times that both the resident and the staff

got hurt. There have been incidents so serious that it has involved one

great danger to his life. After the staff group has received both training and

supervision, the business decided that it is better for the resident to

only have two staff on duty around the clock and they have been working that way since the spring

2014. The staff has noticed that when the resident becomes anxious and shows signs of wanting to hurt yourself, staff or things, it will pass faster if they lets him be alone in his bedroom.

Since the camera was installed, there have been no serious incidents when the resident was alone in the bedroom. The staff was able to quickly pay attention to what he had up to and they also didn't have to disturb when he came to rest. The fact that the camera has been installed does not mean a reduction of the number of personnel on duty; they are always double staffed around the clock.

The camera is only used in real time to see how the resident is doing, nothing material is saved. There is also no sound recording. If the resident wants staff in their room, the staff is there and the camera is not used.

Justification of decisions

Personal data controller

The Social Committee has stated that the Social Committee is responsible for personal data the processing of personal data that has taken place through camera surveillance of a resident in one of the municipality's LSS residences. This is supported by the investigation where it appears that it is the social committee that decided on the camera surveillance and determined purpose and means with the processing of personal data.



What rules apply to camera surveillance

Camera surveillance is a form of personal data processing.

The Camera Surveillance Act (2013:460), which the Social Committee referred to, was replaced on 1 August 2018 by the Camera Surveillance Act (2018:1200) and the

now applies in its place. How and to what extent it is permitted to
camera surveillance is thus regulated in the data protection regulation and
the Camera Surveillance Act (KBL), which supplements the data protection regulation.
Section 2 KBL states that the purpose of the law is to satisfy the need for
camera surveillance for legitimate purposes and to protect natural persons
against undue intrusion into personal integrity during such surveillance.
The definition of camera surveillance in § 3 KBL means, among other things, that it must
be a matter of equipment, which, without being operated on site, is used in a
means that involve long-term or regularly repeated personal surveillance
According to § 7 KBL, a permit is required for camera surveillance of a place there
the public has access, if the monitoring is to be carried out by an authority.
The social welfare committee is an authority and must therefore have as a starting point
permit for camera surveillance of a place to which the public has access. The question is
then if the public is considered to have access to the place that the social committee
camera monitor. It is clear from practice that the term "place where the public has
access" must be interpreted broadly (see the Supreme Administrative Court's decision RÅ 2000 ref.
52).
The Swedish Data Protection Authority's assessment
The Swedish Data Protection Authority states that it is a question of lasting and regular
repeated personal surveillance, with a camera that is not operated on site,
when the social committee uses camera surveillance and films a resident on
an LSS resident, in their bedroom, in real time.
In light of what has emerged about the location of the surveillance, the
resident's bedroom, the Data Inspectorate assesses that it is not a question of a place
to which the public has access. There is thus a requirement to apply for permission
not. The fact that the camera surveillance is permit-free only means that the rules in

the camera surveillance act on permits for camera surveillance does not apply. Other rules in the Camera Surveillance Act apply just as for those subject to a permit camera surveillance, such as rules on confidentiality and information and when



the camera surveillance includes personal data processing, the rules apply in data protection regulation.

Basic principles for processing personal data (Article 5)

Article 5 of the data protection regulation contains a number of basic principles which the personal data controller must take into account when processing personal data.

According to Article 5.2 of the Data Protection Regulation, the personal data controller has responsibility for compliance with the regulation and must be able to demonstrate that they the basic principles are followed.

It follows from Article 5.1 a that all personal data processing must be lawful, correct and characterized by openness. That the treatment must be correct means that it must be fair, reasonable, reasonable and proportionate in relation to them registered.

Article 5.1 c regulates the principle of data minimization, which means that personal data processed be adequate, relevant and not for extensive in relation to the purposes for which they are processed.

It follows from reason 39 that personal data should only be processed for the purpose of the treatment cannot reasonably be achieved by other means.

The Swedish Data Protection Authority's assessment

When assessing whether the treatment is proportionate, the need for

carrying out the processing is weighed against the intrusion into the individual's personal integrity. Regarding the need for the processing, the Data Protection Authority can state that the information that the social committee has provided shows that it The resident's illness creates great difficulties both for him and for others the staff, and that there have been situations where there was a risk of the resident's life and health. It has also happened that staff have arrived damage. The investigation into the matter supports the social committee's assessment that it has there was a need to take measures to manage and improve the situation. The problem that has arisen in the past and that the municipality has managed to curb through the camera surveillance, consists in that when the resident becomes when upset, he is best calmed down by being allowed to withdraw and be himself the bedroom, at the same time as it is then that he is most at risk of injury



himself seriously. There has thus been a need to be able to have the resident under supervision without him being disturbed by the staff.

The Swedish Data Protection Authority notes at the same time that the current camera surveillance means that the resident is monitored by camera in his bedroom. It is therefore a matter of a very privacy-sensitive processing of personal data which means that the resident is monitored in the home's most private sphere. The Swedish Data Protection Authority assesses that the camera surveillance has meant a significant intrusion into it resident's personal integrity.

In order for such surveillance to be deemed an acceptable intrusion into personal integrity, alternative measures must first be excluded.

The Swedish Data Protection Authority notes that the social welfare committee has previously taken measures

in the form of e.g. supervision, to try to improve the situation. It appears
however, not by the investigation that the social committee has tried to fulfill precisely
the need to keep the resident under supervision without the risk of disturbing him,
with less intrusive measures than through camera surveillance. According to
In the Data Inspectorate's assessment, it should be possible for the Social Committee to
with relatively simple and less privacy-intrusive measures
the same needs as with the camera surveillance.
Against this background, the Data Inspectorate finds that the Social Committee has not
demonstrated that the interest in the camera surveillance exceeds the resident's right to
personal integrity and a protected private sphere. The Swedish Data Protection Authority states
that the way in which the camera surveillance was carried out involved an extensive
monitoring of the resident which entailed a significant intervention in the resident's
personal integrity. This means that the processing of personal data, i.e.
the camera surveillance, has been disproportionate in relation to the purpose. The
processing of personal data that took place through the camera surveillance has
thus not meeting the requirements for correctness in Article 5.1 a i
data protection regulation. As the Swedish Data Protection Authority states in the following i
the justification under the headings Legal basis for the processing of
personal data (Article 6), Processing of sensitive personal data (Article
9) and Information to the registered has the processing of personal data
took place without a legal basis in Article 6.1, without support in Article 9.2 and without it being
demonstrated that the resident received information in accordance with Article 13 of the Data Protection Ordinance and not in
accordance with the requirements of the Camera Surveillance Act. The
means that the social committee cannot be considered to have lived up to the requirements in article either
5.1 a of the data protection regulation on legality and transparency.

Legal basis for the processing of personal data (Article 6)

According to Article 5.1 a of the data protection regulation, the personal data must be processed in a legal way. In order for the processing to be considered legal, it is required that at least one of the conditions in Article 6.1 is met.

The Social Committee has stated that the legal basis applicable to it the current personal data processing is that the processing is necessary to perform a task of public interest according to Article 6.1 e i data protection regulation. Provision of social services is one such information of public interest referred to in Article 6.1 e. When it is the question of it the legal basis public interest and exercise of authority may Member States pursuant to Article 6.2 retain or introduce more specific provisions to adapt the application of the provisions of the regulation to national conditions. National law can be closer determine specific requirements for data processing and other measures to ensure legal and fair treatment. But there isn't just one possibility to introduce national rules but also an obligation; article 6.3 states that the basis for the processing referred to in paragraph 1 c and e shall determined in accordance with Union law or the national law of the Member States. The legal basis may also contain special provisions to adapt the application of the provisions of the data protection regulation. Union law or national law of the Member States must fulfill a goal of public interest and be proportionate to the legitimate aim pursued.

This means that supplementary regulations are required in national law through on which the basis for the treatment is established. From reason 41 it appears that such

legal basis or legislative measure should be clear and precise and its

application should be predictable to persons subject to it.

For the processing of personal data in the activities of social services is established

the basis for the processing in Section 6 of the Act (2001:454) on the processing of

personal data within social services (SoLPuL). It is clear from that provision

that personal data may only be processed if the processing is necessary to

tasks within social services must be able to be carried out.

The preparatory work for the Data Protection Act develops what reason 41 means for

supplementary national legislation (prop. 2017/18:105 New data protection act

p. 51).



What degree of clarity and precision is required regarding it

the legal basis for a certain processing of personal data

must be considered necessary in the opinion of the government

is assessed on a case-by-case basis, based on the treatment and

the nature of the business. It should be clear that a treatment of

personal data that does not constitute an actual violation of it

personal integrity, such as with regard to the treatment of

students' names in regular school activities, can be done with the support of a

legal basis that is generally held. A more noticeable intrusion,

for example processing of sensitive personal data in health and

healthcare, requires the legal basis to be more precise

and thus makes the breach foreseeable. If the breach is

significant and involves monitoring or mapping it

the personal circumstances of individuals are also particularly required

statutory support according to ch. 2 §§ 6 and 20 RF.

This means that the requirements of the supplementary national regulation

regarding precision and predictability increases when it is a matter of one more

noticeable intrusion. If the breach is significant and involves surveillance or

mapping of the individual's personal circumstances, which the current one

the processing does, special legal support is also required according to ch. 2 Sections 6 and 20

the form of government.

The Swedish Data Protection Authority's assessment

The Data Inspectorate states that § 6 SoLPuL is a fairly broad and

unspecified provision that forms the basis for processing personal data

in a large number of areas. According to the Data Inspectorate's assessment,

individuals through the provision anticipate that social services treat large

amounts of privacy-sensitive information about individuals in their operations, such as

for example when handling cases. However, it cannot be assumed that

individuals can anticipate that Social Services may also perform

privacy-sensitive camera surveillance. In light of that

the camera surveillance constitutes an extremely privacy-sensitive treatment and that

thus high demands are placed on the national regulation regarding precision and

predictability, the Data Inspectorate considers that the legal basis in § 6

SoLPuL cannot constitute supplementary national provision to it

the legal basis in Article 6.1 e of the Data Protection Regulation when it comes to

privacy-sensitive camera surveillance.

In addition, § 6 SoLPuL requires that the processing is necessary to perform
a job within social services. Regarding the meaning of the term
necessary, the following appears from the preparatory work for the Data Protection Act (prop.
2017/18:105 p. 51).
According to the Swedish Academy's Dictionary, the Swedish word means
necessary that something is absolutely required or cannot
be omitted. However, the concept of Union law does not have this
strict meaning. Requisite of necessity in Article 7 i
the data protection directive has e.g. not considered to constitute a requirement that
it must be impossible to perform a task of public interest
without the treatment measure being taken (prop. 2017/18:105 p. 46).
Although the requirement of necessity does not mean that it must be impossible to perform
a task of public interest if the processing is not carried out, it can
according to the Data Inspectorate's assessment, it is not considered necessary to
carry out an integrity-sensitive processing of personal data via
camera surveillance if there are other reasonable options for carrying one out
task that fulfills the same purpose. As the Swedish Data Protection Authority previously noted
should the social committee also be able to live up to the purpose of the camera surveillance
in a different way than with camera surveillance. This is not the requirement either
on that the treatment must be necessary for the supplementary national
the regulation in § 6 SoLPuL must be applicable fulfilled.
The Social Committee has thus dealt with the camera surveillance
personal data without having a legal basis for the processing according to article
6.1 e of the data protection regulation. Any other legal basis for the processing
according to Article 6.1 has also not been shown to exist.
Processing of sensitive personal data (Article 9)

It follows from Article 9.1 of the data protection regulation that information about health constitutes a special category of personal data (so-called sensitive personal data).

The main rule is that the processing of such personal data is prohibited. IN article 9.2 states a number of exceptions when sensitive personal data may treated.

The Social Committee has stated that the camera may monitor situations in which the resident's illness and state of health appear. It means



that the current camera surveillance at the LSS residence includes treatment of information about health ie. sensitive personal data.

In order for the processing of sensitive personal data to be legal, both are required a legal basis according to Article 6.1 and that any of the exceptions to the prohibition to process sensitive personal data in Article 9.2 is applicable. Already that the fact that the social committee has carried out the camera surveillance without having a legal basis for the processing according to Article 6.1 means that the processing has taken place in violation of Article 9 of the data protection regulation.

If, on the other hand, there had been a legal basis for the processing according to article 6.1, the social committee would thus also need to apply one of the exceptions in Article 9.2 for the processing of personal data to be legal.

Article 9.2 h states that processing of sensitive personal data may take place again the treatment is necessary for reasons related to /…/ social care or management of health and social care services and of their system, on the basis of Union law or national of the Member States right or according to agreements with professionals in the health field and below

provided that the conditions and protective measures referred to in point 3 are

fulfilled.

In order for the exception in Article 9.2 h to be applicable, it is thus required

supplementary rules in Union law or national law. In Swedish law has

the possibility of processing sensitive personal data in social services

activities regulated in § 7 section 3 SoLPuL. From that provision it appears that

sensitive personal data may be processed with the support of Article 9.2 h i

the data protection regulation if the data has been submitted in a case or is

necessary for the business and provided that the requirement for

obligation of confidentiality in Article 9.3 of the data protection regulation is fulfilled.

For the processing of sensitive personal data according to Article 9 of the Data Protection Ordinance, even higher

requirements are placed on the supplementary national

the regulation regarding precision and predictability for it to be

applicable. As the generally designed national regulation cannot be considered

live up to the requirements of precision and predictability and thus constitute

legal basis for processing non-sensitive personal data through

the camera surveillance, nor can it in the corresponding way in general

designed the national provision regarding the treatment of sensitive



personal data is considered to meet the requirements of precision and predictability.

The provision in § 7 SoLPuL cannot therefore constitute such a supplement

national law required for the exception in Article 9.2 h of the Data Protection Regulation to be applicable for the processing of

sensitive personal data

through camera surveillance.

In addition, section 7 SoLPuL also requires that the information has been provided in one matter or are necessary for the business in order for the provision to be able to apply. Since the processing of personal data does not refer to a case but the camera surveillance constitutes an actual act, the data must be necessary for the business so that the processing can be carried out.

Because the necessity requirement cannot, however, be considered fulfilled regarding the requirement for a legal basis for processing personal data, it can nor is it considered to be fulfilled with regard to the exception in Article 9.2 h against the prohibition to process sensitive personal data.

The Swedish Data Protection Authority's assessment

Even if the social committee had a legal basis according to Article 6.1 i data protection regulation, fulfills the processing of personal data through camera surveillance in summary not the requirement for one in Article 9.2 applicable exception to the prohibition against processing sensitive personal data. The Data Inspectorate therefore assesses that Gnosjö municipality by camera monitoring situations where disease picture and state of health has emerged processed sensitive personal data in violation of article 9.1 and 9.2 of the data protection regulation.

Impact assessment and prior consultation (Articles 35 and 36)

It follows from Article 35 of the Data Protection Regulation that a personal data controller i in some cases, a consequence assessment must be made regarding data protection, i.e. before the processing of personal data make an assessment of a planned processing consequences for the protection of personal data. The obligation applies about a type of treatment, especially with the use of new technology and with taking into account its nature, scope, context and purpose, likely leads to a high risk for the rights and freedoms of natural persons.

Article 35.7 shows what an impact assessment must contain. It will

at least include a description of the planned treatment and

the purposes of the processing, an assessment of the need for and proportionality

with the processing, an assessment of the risks to the data subjects' rights



and freedoms as well as the measures planned to manage the risks and show that

the data protection regulation is complied with.

An impact assessment can thus be described as a tool to

identify risks with the processing of personal data and develop routines

and measures to manage the risks, and thus assess the treatment

is proportionate to its purpose. To implement a

impact assessment before starting the treatment is thus often an important one

measure to assess whether a treatment is legal.

According to Article 36, the personal data controller must consult with

The Swedish Data Protection Authority prior to the processing of an impact assessment regarding

data protection according to Article 35 shows that the processing would lead to a high risk

unless the controller takes measures to reduce the risk.

The European Data Protection Board, EDPB3, has produced guidelines4 regarding i

which situations a treatment is likely to lead to a high risk of physical

people's freedoms and rights. The guidelines specify nine criteria that must be taken into account

when assessing whether a processing of personal data is likely to lead to

a high risk for the data subject. If two of the criteria are met, it can

personal data controllers in most situations assume that a

impact assessment must be carried out, but also a treatment that only

meets one of these criteria may in some cases require an impact assessment.

Conversely, two or more of the criteria in the guidance may be met but

the personal data controller can still make the assessment that the processing

unlikely to lead to a high risk for the data subject's freedoms and rights. IN

such situations, the data controller should justify and

document the reasons why an impact assessment is not carried out and

include the views of the data protection officer.

The Data Protection Authority has, guided by guidelines from the Article 29 working group and the criteria developed by the

group, decided a

list of personal data processing covered by requirements for

impact assessment regarding data protection (2019-01-16, dnr DI-2018-13200).

The list supplements and specifies article 35.1 and is intended to

European Data Protection Board, formerly the Article 29 Group.

Guidelines on impact assessment regarding data protection and determining whether

the processing is "likely to lead to a high risk" in the sense referred to in the regulation

2016/679, WP 248 rev. 01.

3

4



further exemplify when the conditions in that provision can be considered

be fulfilled. The list is not intended to be exhaustive

when an impact assessment must be carried out. Criteria to be considered at

the assessment of whether a planned treatment is likely to lead to high risk is

among other things, if the processing refers to the systematic monitoring of people,

sensitive data or data of a very personal nature, data about
vulnerable people or the use of new technology or new organizational
solutions.
An impact assessment must be carried out on at least two of those on the list
the listed points are included in the planned treatment. It is
only mandatory to carry out an impact assessment if the planned
the processing "is likely to lead to a high risk for the rights of natural persons
and freedoms". A treatment may meet two or more of the criteria but it
the personal data controller can still make the assessment that it is likely not
leads to a high risk. In such situations, the personal data controller should
justify and document the reasons why an impact assessment
not carried out and include the views of the data protection officer. In the end of
The Data Inspectorate's list also gives examples of when at least two of
the criteria must be considered present and thus when an impact assessment
must be made. Examples include when activities within social care
uses camera surveillance in people's homes.
The Social Committee has stated that they have not made any impact assessment
because they do not save information from the camera surveillance. Social Committee
has also not come in with any request for prior consultation
The Swedish Data Protection Authority.
The Swedish Data Protection Authority's assessment
The Data Inspectorate states that criteria to be taken into account in the assessment
of whether a treatment is likely to lead to high risk is if the treatment refers
systematic surveillance of people, sensitive data or data of
highly personal nature, information about vulnerable people or application of
new technology or organizational solutions.

From the Data Inspectorate's list it appears that when activities within social

care uses welfare technology, e.g. robots or camera surveillance, i

people's housing, then it is an example of treatment that requires a

impact assessment is carried out. Then the criteria are considered to be in effect systematically



monitoring, processing of sensitive personal data and use of new

technology or new organizational solutions be fulfilled.

According to the Data Inspectorate's assessment, the current processing has included

a number of criteria that indicate that the treatment is likely to lead to a high

risk to the rights and freedoms of the data subject. An explicit example i

The Swedish Data Protection Authority's list of when impact assessment is required according to

the data protection regulation is when activities within social care, as in this

case, uses camera surveillance in people's residences. Then the social committee does not

has explained its assessment not to carry out an impact assessment

has it not shown that the treatment is unlikely to lead to a high risk, even though

several of the criteria in the guidelines are met. According to the Swedish Data Protection Authority

assessment, the social committee has thus processed personal data in violation of

Article 35 of the Data Protection Regulation.

Based on what has emerged in the case, the Social Committee has not either

came in with a prior consultation. Because the social committee has not done any

impact assessment, there has also been no assessment of whether

the processing entailed some risks for the rights and freedoms of the data subject.

Thus, the social committee has also not been able to show that the high risk which

likely to exist has been lowered in such a way that there has been no reason

to request prior consultation with the Data Protection Authority. According to the Swedish Data Protection Authority

The Social Committee's processing of personal data therefore also has an assessment

took place in violation of Article 36 of the Data Protection Regulation.

Information to registered users

Article 13 of the data protection regulation states which information must

provided if personal data is collected from the data subject, such as

information about the identity and contact details of the personal data controller, the purposes of the processing for which the

personal data is

intended, the legal basis, the period during which the personal data

will be stored as well as the data subject's rights.

Article 12 of the data protection regulation states that it

personal data controller must take appropriate measures to to it

data subjects provide all the information referred to in Article 13, and that such

information must be provided in a concise, clear, clear, comprehensible and easy manner

accessible form and using clear and unambiguous language.

The information must be provided in writing or in some other form. For reasons



58 of the data protection regulation states that information must be concise,

easily accessible and easy to understand and designed in clear and simple language

and that, if necessary, visualization is used.

The Social Committee has stated that they provided oral information to it

resident, the resident's manager and relatives. Also staff and visitors

is said to have received information about the camera surveillance.

Regarding the information provided to the resident, the Social Committee has

stated that the resident has received information about the camera surveillance through
that he was there and watched when the camera was installed, and that the manager
verbally explained to the resident that the purpose of the camera is to staff
must know that the resident is well. It has not emerged that in addition
given some other information about the camera surveillance to the resident.

The Swedish Data Protection Authority notes that the information provided by the social welfare committee
to the registered (resident) only includes information that
camera surveillance is going on, and not all the information that it
personal data controller is obliged to provide to the registered at
collection of personal data in accordance with Article 13 of the Data Protection Regulation.

The Social Committee has also stated that information has been provided to it
registered administrator. It appears from chapter 11, chapter 4 and §§ 7 of the Parental Code (1949:381)
that the court may appoint an administrator for the person who, due to illness,
mental disorder, weakened state of health or similar condition needs
help with guarding one's rights, managing one's property or providing for one's person,
and it is not enough that a good man is appointed or that the individual on
some other less invasive way will help. The trustee assignment must be adapted
to the individual's needs in each particular case and may be limited to refer to certain
property or matter.

The Swedish Data Protection Authority notes that even when an administrator's assignment is designed
in such a way that it includes the task of providing for the person of the individual exists
it limits what a trustee is allowed to do. Of the preparatory work to
the regulations on stewardship appear as follows.

In general, the principal should also be allowed to decide matters himself
relating to his accommodation as well as the content of care offered. One
Trustees should therefore not normally represent the principal

when it comes to issues of consent to, for example, operative interventions.

Of course, this does not prevent one from i.a.

care facilities' side obtains the administrator's views (prop.

1987/88:124 p 172).

In the request for completion, the Swedish Data Protection Authority has sent on 15 June 2020

urged the social committee to provide documentation to the Data Inspectorate regarding

the scope of the trustee assignment and what information has been provided to

the trustee. However, the Social Committee has not received the documentation

regarding the scope of the trustee assignment and has not provided an account of either

what information has been provided to the trustee. In addition, the Social Committee has

nor explained its assessment that the administrator can represent it

resident regarding his right to information according to Article 13 i

data protection regulation.

The Swedish Data Protection Authority's assessment

The Social Committee has not shown that there is an opportunity to inform

the administrator, instead of the person registered in the current case, or that it

information that appears in Article 13 of the Data Protection Regulation has been provided.

The Social Committee has thus not fulfilled the obligation to provide information by

inform the administrator. Then neither is the information that the social committee has

given to the resident is sufficient for the information obligation to be

fulfilled, the social committee's processing of personal data has also taken place in violation

with Article 13 of the Data Protection Regulation.

Furthermore, it appears from § 15 of the Camera Surveillance Act (KBL) that information about

camera surveillance must be provided by clear signage or on something else

effective way. It also appears that regulations on the right to

information about the personal data processing such as the camera surveillance

means can be found in the data protection regulation and other regulations specified in § 6

KBL.

The Social Committee has not provided information that there is any sign that

informs that camera surveillance is being carried out. For the social committee to be considered

have lived up to the requirements regarding information in the Camera Surveillance Act must

thus, information about camera surveillance is considered to have been left on something else

effective way.



As stated above, the information about the camera surveillance lives as

the social committee states that it has not submitted the requirements for information

according to the data protection regulation. The Swedish Data Protection Authority further assesses that

the social committee also did not live up to the requirements to provide information about

camera surveillance in other effective ways. This means that the treatment of

personal data also occurred in violation of the requirement for information in § 15 KBL.

Because the resident has not received prescribed information according to

the data protection regulation nor according to the camera surveillance act can

the social committee is not considered to have met the requirements for openness in Article 5.1 a i

data protection regulation.

Choice of intervention

Legal regulation

If there has been a breach of the data protection regulation has

Datainspektionen a number of corrective powers to be available according to article 58.2 a–j of the data protection regulation. The supervisory authority can, among other things order the personal data controller to ensure that the processing takes place in in accordance with the regulation and if required in a specific manner and within a specific period.

It follows from Article 58.2 of the data protection regulation that the Data Inspectorate in accordance with Article 83 shall impose penalty charges in addition to or instead of others corrective measures referred to in Article 58(2), depending on the circumstances in each individual case.

For authorities, according to Article 83.7 of the Data Protection Regulation, national rules state that authorities can impose administrative penalty fees.

According to ch. 6 § 2 of the Data Protection Act, penalty fees can be decided for authorities, but to a maximum of SEK 5,000,000 alternatively SEK 10,000,000 depending on whether the violation relates to articles covered by Article 83(4) or 83.5 of the data protection regulation. Section 25 point 4 KBL also states that a penalty fee can be charged to the person who operates camera surveillance and violates against the information requirement in § 15.

Article 83(2) sets out the factors to be taken into account in deciding whether a administrative penalty fee shall be imposed, but also what shall affect the amount of the penalty fee. Of central importance for the assessment of



the seriousness of the breach is its nature, severity and duration. About it is a question of whether a minor violation gets the supervisory authority, according to reason 148 i data protection regulation, issue a reprimand instead of imposing one

penalty fee.

Penalty fee

The Data Inspectorate's supervision has shown that the Social Committee has processed

personal data in violation of articles 5, 6.1, 9.2, 13, 35 and 36 of

data protection regulation. In addition, the social committee has violated § 15 KBL.

When assessing whether the violations are so serious that an administrative

penalty fee must be imposed, the Data Inspectorate has taken into account that

the processing of personal data intended for camera surveillance of a resident in a

very private sphere and in a dependent position, where the treatment to some extent

covered sensitive personal data. The treatment has been ongoing from March 2019 to April 2020, which is considered a

relatively long time. Consideration has also been given

that the Data Protection Authority has become aware of the processing through a tip from

a relative of the registered person. These circumstances are seen as aggravating.

According to the Data Inspectorate's assessment, the processing has not involved a

minor violation without violations that will lead to an administrative

penalty fee.

Then the articles in the data protection regulation that the social committee violated

is covered by Article 83.5 of the data protection regulation and refers to a violation

of the disclosure obligation in § 15 KBL is the maximum amount for

the sanction fee in this case SEK 10 million, according to ch. 6 Section 2, second paragraph

the law (2018:218) with supplementary provisions to the EU's

data protection regulation.

The administrative penalty fee must be effective, proportionate and

deterrent. This means that the amount must be determined so that it

the administrative sanction fee leads to correction, that it provides a preventive measure

effect and that it is also proportionate in relation to current as well

violations as to the solvency of the subject of supervision.

In determining an amount that is effective, proportionate and

discouragingly, the Data Inspection Authority can state that the social welfare committee has

processed sensitive personal data about a resident in a situation that is very

private and which means that the residents are in a dependent position



against the municipality. The violation refers to the surveillance of a person in his

bedroom, which is a very privacy-infringing treatment. In addition, have

the treatment has been going on for a relatively long time, for more than a year. The Swedish Data Protection Authority

have taken into account that residents have serious self-harming behaviour,

sometimes with danger to life and health both for himself and the staff.

The Social Committee has taken the measure to resolve a complex situation there

staff and residents have risked injury. Although the situation

has been difficult to manage, the social committee has not tried alternatives, less

intervention measures to solve the problem of being able to have the resident

under supervision in a smooth manner before the camera surveillance began.

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

the penalty fee must be effective, proportionate and dissuasive

The Swedish Data Protection Authority that the administrative sanction fee for the social welfare committee

shall be determined at SEK 200,000.

This decision has been made by the director general Lena Lindgren Schelin after

presentation by lawyer Jeanette Bladh Gustafson. At the final

the handling is also handled by chief legal officer Hans-Olof Lindblom and

unit managers Malin Blixt and Charlotte Waller Dahlberg participated.

Lena Lindgren Schelin, 2020-11-24 (This is an electronic signature)

Appendix

How to pay penalty fee

Copy for the attention of:

Data protection representative for Gnosjö municipality: dataskyddsombud@gislaved.se

How to appeal

If you want to appeal the decision, you must write to the Swedish Data Protection Authority. Enter in the letter which decision you are appealing and the change you are requesting.

The appeal must have been received by the Swedish Data Protection Authority no later than three weeks from the day the decision was announced. If the appeal has been received in time





the Swedish Data Protection Authority forwards it to the Administrative Court in Stockholm for examination.

You can e-mail the appeal to the Swedish Data Protection Authority if it does not contain any privacy-sensitive personal data or information that may be covered by secrecy. The authority's contact details appear on the first page of the decision.