

Decision

Diarienn

2020-11-24

DI-2019-7782

Gnosjö Municipality - Social Affairs Committee

Supervision according to the EU Data Protection Regulation

2016/679 - camera surveillance at an LSS accommodation

Table of Contents

The Data Inspectorate's decision	3
Administrative penalty fees	3
Report on the supervisory matter	4
Background.....	4
What has emerged in the case	4
Motivation for decision	5
Personal data controller	5
What rules apply to camera surveillance	6
The Data Inspectorate's assessment	6
Basic principles for the processing of personal data (Article 5)	7
The Data Inspectorate's assessment	7
Legal basis for the processing of personal data (Article 6)	9
The Data Inspectorate's assessment	10
Processing of sensitive personal data (Article 9)	11
The Data Inspectorate's assessment	13
Impact assessment and prior consultation (Articles 35 and 36)	13
The Data Inspectorate's assessment	15
Information for registered	16

The Data Inspectorate's assessment	18
Choice of intervention	19
Legal regulation	19
Penalty fee	20

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Phone: 08-657 61 00

1 (22)

The Data Inspectorate

DI-2019-7782

Appendix	21
----------------	----

Copy for information to:	21
--------------------------------	----

How to appeal.....	21
--------------------	----

2 (22)

The Data Inspectorate

DI-2019-7782

The Data Inspectorate's decision

The Data Inspectorate states that Gnosjö Municipality - Social Affairs Committee below

the period March 2019 - April 2020, the camera monitored a resident of an LSSboende¹ in her 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 treatment of

personal data ie. not been legal. That the camera surveillance has been performed

in a way that is more intrusive to the resident's privacy

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

the purpose, ie. did not live up to the requirements of accuracy as well as that the camera surveillance took place without the resident being prescribed information either under the Data Protection Regulation or the Camera Surveillance Act, ie. 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 on disease and health condition without having legal support for it the treatment,

Articles 35 and 36 by failing to meet the requirements of a impact assessment and not have prior consultation with

The Data Inspectorate and

Article 13 by failing to comply with the information requirement registered (the resident) as well

§ 15 of the Camera Surveillance Act (2018: 1200) by not having left information about the camera surveillance through clear signage or on any other effective way.

Administrative penalty fees

The Data Inspectorate decides by decision pursuant to Articles 58 (2) and 83 i the Data Protection Ordinance, Chapter 6 Section 2 of the Act (2018: 218) with supplementary provisions of the EU Data Protection Regulation and § 25 point 4 i

Camera Surveillance Act (2018: 1200) that Gnosjö Municipality - Social Affairs Committee for

1

Housing with special service according to law (1993: 387) on support and service to some handicapped.

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

on the protection of individuals with regard to the processing of personal data and on that free flow of such data and repealing Directive 95/46 / EC (General Data Protection Regulation).

3 (22)

The Data Inspectorate

DI-2019-7782

infringements 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.

Report on the supervisory matter

Background

On 2 May 2019, the Data Inspectorate received a report from another relative a resident of an LSS residence in Gnosjö municipality according to which the social committee in Gnosjö municipality (hereinafter the social committee) processes personal data through to camera monitor a resident at one of the municipality's LSS homes. 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 of the resident. There is no approval / consent according to the submitter of the notification.

Due to the information contained in the notification, the Data Inspectorate has initiated supervision for the purpose 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 rules and the camera surveillance law.

The supervisory case began with a supervisory letter on 15 July 2019. Answer to

The supervisory letter was received on 21 August 2019. Supplementary letters from

The Social Affairs Committee has been received on 2 December 2019, 11 May 2020, 12

August 2020 and November 4, 2020.

What has emerged in the case

The Social Affairs Committee has processed personal data by real-time camera monitor a resident of an LSS residence in order to increase its security accommodation. The camera was installed in March 2019 and surveillance ceased on the 29th April 2020 in connection with the operation being taken over by another contractor.

The Social Affairs Committee has stated the following. The resident has lived in the LSS accommodation since the autumn of 2013. He needs support in his everyday life around the clock from two people, when he exposes himself to serious self-harming behavior and needs help to prevent this. In emotionally difficult situations, he wants to be himself in his own bedroom with closed door, the staff has then been in the living room and been prepared to enter if necessary. It has happened that it has become completely quiet inside

4 (22)

The Data Inspectorate

DI-2019-7782

at the resident's and when staff have opened the door to see how they are doing he slept but woke up when the door was opened. The resident has then again become emotionally upset and risk of self-harming behavior has been present. At others On several occasions, 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 staff members service, despite this, it happened several times to both the resident and the staff was injured. There have been such serious incidents that it has involved one great danger to her life. After the staff group has received both training and guidance, 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 since the spring

2014. The staff has noticed that when the resident becomes anxious and shows signs of wanting to harm themselves, staff or things, it passes more quickly if they lets him be alone in his bedroom.

Since the camera was installed, there have been no serious incidents when the resident has been alone in the bedroom. The staff was able to quickly pay attention to what he had in mind and they have not had to disturb when he came to rest. The fact that the camera is installed does not mean a reduction of the number of staff in service; they are always double-staffed around the clock. The camera is only used in real time to see how the resident is feeling, nothing material is saved. There is also no sound recording. If the resident wants staff inside their room, the staff is there and the camera is not used.

Justification of decision

Personal data manager

The Social Affairs Committee has stated that the Social Affairs Committee is responsible for personal data the processing of personal data that has taken place through camera surveillance of a residence in one of the municipality's LSS residences. This is supported by the inquiry where it appears that it is the Social Affairs Committee that decides on camera surveillance and specific purpose and means with personal data processing.

5 (22)

The Data Inspectorate

DI-2019-7782

What rules apply to camera surveillance

Camera surveillance is a form of personal data processing.

The Camera Surveillance Act (2013: 460), to which the Social Affairs Committee referred, 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 allowed to

camera surveillance is thus regulated in the Data Protection Regulation and

the Camera Surveillance Act (KBL), which complements the Data Protection Ordinance.

Section 2 of the KBL states that the purpose of the law is to meet the need for

camera surveillance for legitimate purposes and to protect natural persons

against undue invasion of privacy during such surveillance.

The definition of camera surveillance in § 3 KBL means, among other things, that it should

be a matter of equipment, which without being maneuvered on site, is used on one

means involving permanent or regular repeated personal surveillance

According to § 7 KBL, a permit is required for camera surveillance of a place where

the public has access, if the surveillance is to be conducted by an authority.

The Social Affairs Committee is an authority and must therefore have as a starting point

permission to camera-monitor a place to which the public has access. The question is

then if the public is considered to have access to the seat of the Social Affairs Committee

camera guards. Practice shows that the concept of "place where the public has

access" shall be interpreted broadly (see the Supreme Administrative Court's decision RÅ 2000 ref.

52).

The Data Inspectorate's assessment

The Data Inspectorate states that this is a permanent and regular issue

repeated personal surveillance, with a camera that is not operated on the spot,

when the social committee uses camera surveillance and films a resident

an LSS home, in his bedroom, in real time.

In the light of what has emerged about the place of surveillance, it

living room, 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 a permit

not. The fact that the camera surveillance is unlicensed only means that the rules in

the Camera Surveillance Act on Camera Surveillance Permits 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 professional secrecy and information and when

6 (22)

The Data Inspectorate

DI-2019-7782

the camera surveillance includes personal data processing, the rules in the Data Protection Regulation.

Basic principles for the processing of personal data (Article 5)

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

According to Article 5 (2) of the Data Protection Regulation, the data controller has responsibility for compliance with the Regulation and must be able to demonstrate that they basic principles are followed.

It follows from Article 5 (1) (a) that all processing of personal data must be lawful; correct and characterized by openness. That the treatment must be correct means that it should be fair, equitable, reasonable and proportionate in relation to them registered.

Article 5 (1) (c) regulates the principle of data minimization, which means that: personal data processed to be adequate, relevant and not for extensive in relation to the purposes for which they are treated.

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

The Data Inspectorate's assessment

In assessing whether the treatment is proportionate, the need for

to carry out the treatment is weighed against the intrusion into the individual's personal integrity. Regarding the need for processing, the Data Inspectorate can note that the information provided by the Social Affairs Committee shows that it residents' illness creates great difficulties both for themselves and for staff, and that situations have arisen where there has been a risk of the resident's life and health. It has also happened that staff have been added damage. The inquiry into the case supports the Social Affairs Committee's assessment that it has there has been a need to take action to manage and improve the situation. The problem that has arisen before and that the municipality has managed to curb through the camera surveillance, consists in that when the resident becomes upset is calmed down best by being allowed to retreat and be alone in the bedroom, while at the same time there is the greatest risk of him injuring himself

7 (22)

The Data Inspectorate

DI-2019-7782

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

At the same time, the Data Inspectorate finds that the current camera surveillance means that the resident is monitored by a camera in his bedroom. It is thus a question of a very privacy-sensitive processing of personal data which means that the resident is monitored in the home's most private sphere. The Data Inspectorate assesses that the camera surveillance has entailed a significant intrusion into it resident's privacy.

In order for such surveillance to be judged to be an acceptable intrusion into personal integrity, alternative measures must first be ruled out.

The Data Inspectorate notes that the Social Affairs Committee has previously taken measures

in the form of e.g. guidance, to try to improve the situation. It appears however, not by the inquiry that the Social Affairs Committee has tried to fulfill precisely the need to keep the resident under surveillance without risking disturbance; with less intrusive measures than through camera surveillance. According to The Data Inspectorate's assessment should be possible for the Social Affairs Committee to with relatively simple and less intrusive measures same needs as with camera surveillance.

Against this background, the Data Inspectorate finds that the Social Affairs Committee does not have shown that the interest in the camera surveillance exceeds the resident's right to privacy and a protected private sphere. The Data Inspectorate states that the way in which the camera surveillance was carried out entailed an extensive monitoring of the resident which has led to a significant intervention in the resident privacy. This means that the processing of personal data, ie. camera surveillance, has been disproportionate to the purpose. The processing of personal data that has taken place through the camera surveillance has thus not complied with the requirements of correctness in Article 5 (1) (a) (i) the Data Protection Regulation. As the Data Inspectorate states in the following in the justification under the headings Legal basis for the treatment of personal data (Article 6), Processing of sensitive personal data (Article 9) and Information to the data subjects has the processing of personal data without a legal basis in Article 6 (1), without support in Article 9 (2) and without demonstrated that the resident has received information in accordance with Article 13 of the Data Protection Ordinance and also not in accordance with the requirements of the Camera Surveillance Act. The means that the Social Affairs Committee can also not be considered to have lived up to the requirements in Article 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, personal data must be processed in a legal way. In order for the treatment to be considered legal, it is required that at least one of the conditions of Article 6 (1) is met.

The Social Affairs 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 general interest in accordance with Article 6 (1) (e) (i)

the Data Protection Regulation. The provision of social services is one such information of general interest referred to in Article 6 (1) (e)

the legal basis of general interest and the exercise of authority

Member States in accordance with Article 6 (2) maintain or introduce more specific provisions to adapt the application of the provisions of

Regulation to national circumstances. National law can be closer

establish specific requirements for data processing and other measures to:

ensure legal and fair treatment. But there is not just one

possibility to introduce national rules but also an obligation; Article 6.3

states that the basis for the treatment referred to in paragraph 1 (c) and (e) shall be:

determined in accordance with Union law or the national law of the Member States.

The legal basis may also contain specific provisions to:

adapt the application of the provisions of the Data Protection Regulation.

The law of the Union or the national law of the Member States shall fulfill an objective of:

public interest and be proportionate to the legitimate aim pursued.

This means that additional provisions in national law are required by

which the basis for the treatment is determined. Recital 41 states that one

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

application should be predictable for persons covered by it.

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

the basis for the treatment in section 6 of the Act (2001: 454) on the treatment of

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

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

tasks within the social services must be able to be performed.

The preparatory work for the Data Protection Act develops what recital 41 entails

supplementary national legislation (Bill 2017/18: 105 New data protection law

p. 51).

9 (22)

The Data Inspectorate

DI-2019-7782

What degree of clarity and precision is required in terms of it

legal basis for a certain processing of personal data

should be considered necessary must in the opinion of the Government

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 in the treatment of

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

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

for example processing of sensitive personal data in health and

healthcare, requires that the legal basis be more precise

thus making the intrusion predictable. If the intrusion is

significant and involves monitoring or mapping it

In addition, the personal circumstances of the individual are specifically required legal support according to ch. 26 and 20 §§ RF.

This means that the requirements for the supplementary national regulation in terms of precision and predictability increases when it comes to one more tangible intrusion. If the intrusion is significant and involves monitoring or mapping of the individual's personal circumstances, which the current the treatment does, special legal support is also required according to ch. Sections 6 and 20 the form of government.

The Data Inspectorate's assessment

The Data Inspectorate finds that § 6 SoLPuL is a fairly broad and unspecified provision which forms the basis for the processing of personal data in a large number of areas. According to the Swedish Data Inspectorate's assessment, individuals by the provision anticipate that the social services treat large amounts of privacy-sensitive information about individuals in their business, such as for example in case processing. However, it can not be assumed that individuals can anticipate that the Social Services may also perform privacy-sensitive camera surveillance. Against the background of that the camera surveillance constitutes an extremely privacy-sensitive treatment and that it thus, high demands are placed on national regulations regarding precision and predictability, the Data Inspectorate assesses that the legal basis in § 6 SoLPuL cannot constitute a supplementary national provision to it the legal basis of Article 6 (1) (e) of the Data Protection Regulation in this case privacy-sensitive camera surveillance.

10 (22)

The Data Inspectorate

DI-2019-7782

In addition, § 6 SoLPuL requires that the treatment is necessary to perform a task within the social services. Regarding the meaning of the term necessary, the following appears from the preparatory work for the Data Protection Act (Bill. 2017/18: 105 p. 51).

According to the Swedish Academy's Dictionary, the Swedish word means necessary that something absolutely required or can not omitted. However, the concept of Union law does not have this strict meaning. Necessity requisites in Article 7 i

The Data Protection Directive has e.g. was not considered to be a requirement that it must be impossible to perform a task of general interest without the treatment measure being taken (Bill 2017/18: 105 p. 46).

Even if the requirement of necessity does not mean that it should be impossible to perform a task of general interest if the treatment is not carried out, it can according to the Data Inspectorate's assessment is not considered necessary to carry out a privacy-sensitive processing of personal data via camera surveillance if there are other reasonable options for performing one task that serves the same purpose. As the Data Inspectorate previously stated the social committee should be able to live up to the purpose of the camera surveillance in a different way than with just camera surveillance. Thus, neither is the requirement that the treatment shall be necessary for the complementary national the regulation in § 6 SoLPuL shall be applicable fulfilled.

The Social Affairs Committee has thus dealt with the camera surveillance personal data without having a legal basis for the processing under Article 6.1 e of the Data Protection Regulation. Any other legal basis for the treatment under 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 health data constitute 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) sets out a number of exceptions for sensitive personal data treated.

The Social Affairs Committee has stated that the camera may monitor situations in which the resident's disease picture and state of health appear. It means
1 1 (22)

The Data Inspectorate

DI-2019-7782

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

In order for a processing of sensitive personal data to be legal, both are required a legal basis under Article 6 (1) and that any of the exceptions to the prohibition the processing of sensitive personal data in Article 9 (2) is applicable. Already it the fact that the Social Affairs Committee has carried out the camera surveillance without having a legal basis for the proceedings under Article 6 (1) means that processing has been carried out in breach of Article 9 of the Data Protection Regulation.

If, on the other hand, there had been a legal basis for the treatment under Article 6.1, the Social Affairs Committee would thus also have had to apply some of the exceptions in Article 9 (2) for the processing of personal data to be lawful.

Article 9 (2) (h) provides that the processing of sensitive personal data may be repeated the treatment is necessary for reasons related to /... / social care or management of health services and social care and by their systems, on the basis of Union law or the national law of the Member States right or under agreements with health professionals and under

provided that the conditions and safeguard measures referred to in paragraph 3 are fulfilled.

In order for the derogation in Article 9 (2) (h) to apply, it is therefore necessary supplementary rules of Union or national law. In Swedish law has the possibility of processing sensitive personal data in the social services activities are regulated in § 7 3 st SoLPuL. It is clear from that provision that sensitive personal data may be processed pursuant to Article 9 (2) (h) of (i) the Data Protection Regulation if the information has been provided in a case or is necessary for the business and provided that the requirement of confidentiality in Article 9 (3) of the Data Protection Regulation is fulfilled.

The processing of sensitive personal data in accordance with Article 9 of the Data Protection Regulation thus places even higher demands on the the regulation regarding precision and predictability for it to be applicable. Then the generally formulated national regulation can not be considered live up to the requirements of precision and predictability and thus constitute legal basis for the processing of non-sensitive personal data by camera surveillance, nor can it in a similar way in general drafted the national provision on the treatment of sensitive

1 2 (22)

The Data Inspectorate

DI-2019-7782

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

The provision in § 7 SoLPuL can thus not constitute such a supplement national law necessary for the application of the derogation in Article 9 (2) (h) of the Data Protection Regulation to the processing of sensitive personal data; through camera surveillance.

In addition, section 7 of SoLPuL also requires that the information has been submitted in one case or are necessary for the business for the provision to be able to apply. Then the processing of personal data does not refer to a case but camera surveillance is an actual act, the information must be necessary for the activity may be that the treatment can be performed. However, since the requirement of necessity can not be considered fulfilled regarding the requirement of a legal basis for the processing of personal data, it may is also not considered to be fulfilled with regard to the exemption in Article 9 (2) (h) against the ban on the processing of sensitive personal data.

The Data Inspectorate's assessment

Even if the Social Affairs Committee had a legal basis under Article 6 (1) (i) the Data Protection Regulation, fulfills the processing of personal data by

In summary, camera surveillance does not require one in Article 9 (2)

applicable exemption from the ban on treating sensitive

personal data. The Data Inspectorate thus assesses that Gnosjö municipality

by camera-watching situations where the disease picture and health condition

sensitive data has been processed in breach 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 data controller in some cases must make an impact assessment regarding data protection, ie. before the processing of personal data make an assessment of a planned processing consequences for the protection of personal data. The obligation applies on a type of treatment, in particular with the use of new technologies and with taking into account its nature, scope, context and purpose, is likely to lead to a high risk to the rights and freedoms of natural persons.

Article 35 (7) sets out what an impact assessment should include. It will at least include a description of the planned treatment and purposes of the treatment, an assessment of the need for and proportionality in the processing, an assessment of the risks to the data subjects' rights

13 (22)

The Data Inspectorate

DI-2019-7782

and freedoms as well as the measures planned to manage the risks and demonstrate that the Data Protection Regulation is complied with.

An impact assessment can thus be described as a tool for 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 one impact assessment before starting treatment is thus often an important one action to assess whether a treatment is lawful.

According to Article 36, the controller shall consult:

The Data Inspectorate before the processing of an impact assessment regarding data protection under Article 35 shows that the processing would lead to a high risk unless the data controller takes measures to reduce the risk.

The European Data Protection Board, EDPB³, has developed guidelines⁴ regarding i what situations a treatment is likely to lead to a high risk of physical freedoms and rights of persons. The guidelines set out nine criteria that must be taken into account in 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 controller in most situations assume that a impact assessment should be performed, 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 guide may be met but

the data controller can still make the assessment that the processing

probably does not lead to a high risk to the data subject's freedoms and rights. IN

such situations, the 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 Inspectorate has, on the basis of guidelines from Article 29 of the Working Group and the criteria developed by the Group,

list of personal data processing covered by requirements for

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

The list complements and specifies Article 35 (1) and is intended to:

European Data Protection Board, former Article 29 Working Party.

Guidelines on data protection impact assessment and determination of whether

the treatment "is likely to lead to a high risk" within the meaning of the Regulation

2016/679, WP 248 rev. 01.

3

4

1 4 (22)

The Data Inspectorate

DI-2019-7782

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 needs to be made. Criteria to be considered in

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

including whether the treatment concerns systematic monitoring of humans,

sensitive data or data of a very personal nature, data on vulnerable persons or the use of new technology or new organizational solutions.

An impact assessment must be made of at least two of those on the list the listed points are included in the planned treatment. It is only mandatory to perform an impact assessment on the planned the treatment "is likely to lead to a high risk to the rights of natural persons and freedoms ". A treatment can meet two or more of the criteria but it personal data controller can still make the assessment that it is unlikely to leads to a high risk. In such situations, the person responsible for personal data should justify and document the reasons for an impact assessment not performed and include the views of the Data Protection Officer. In the end of The Data Inspectorate's list is also given examples of when at least two of the criteria shall be considered to exist and thus when an impact assessment must be made. Examples are given when activities in social care uses camera surveillance in people's homes.

The Social Affairs Committee has stated that they have not made any impact assessment because they do not save information from the camera surveillance. The Social Affairs Committee has also not submitted any request for prior consultation The Data Inspectorate.

The Data Inspectorate's assessment

The Data Inspectorate states that criteria that must be taken into account in the assessment of whether a treatment is likely to lead to a high risk is whether the treatment is intended systematic monitoring of people, sensitive data or data of very personal in nature, information on vulnerable persons or the application of new technology or organizational solutions.

The Data Inspectorate's list shows that when activities within social care uses welfare technology, e.g. robots or camera surveillance, in people's housing, it's an example of treatment that requires one impact assessment is performed. Then the criteria are considered systematic

15 (22)

The Data Inspectorate

DI-2019-7782

monitoring, processing of sensitive personal data and use of new technology or new organizational solutions must be met.

According to the Data Inspectorate's assessment, the treatment in question has included a number of criteria suggest that the treatment is likely to lead to a high risk to the data subject's freedoms and rights. An explicit example in

The Data Inspectorate's list of when impact assessment is required according to

The Data Protection Regulation is when activities in social care, as in this cases, use camera surveillance in people's homes. Then the Social Affairs Committee does not has presented its assessment of not carrying out an impact assessment

it has not shown that the treatment is unlikely to lead to a high risk, despite the fact that several of the criteria in the guidelines are met. According to the Data Inspectorate assessment, the Social Affairs 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 Affairs Committee has not either submitted with a prior consultation. Because the Social Affairs Committee did not do any impact assessment, no assessment has been made of whether the processing entailed some risks to the data subject's freedoms and rights.

Thus, the Social Affairs Committee has also not been able to show that the high risk that likely to have been lowered in such a way that there has been no reason

to request prior consultation with the Data Inspectorate. According to the Data Inspectorate assessment, the social committee's processing of personal data thus also has in breach of Article 36 of the Data Protection Regulation.

Information for registered

Article 13 of the Data Protection Regulation sets out the information to be provided

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

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

the data controller shall take appropriate measures to enable it

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

information must be provided in a concise, clear, concise, comprehensible and easy available form and using clear and distinct language.

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

16 (22)

The Data Inspectorate

DI-2019-7782

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 Affairs Committee has stated that they provided oral information to it

residents, the resident's trustees 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 Affairs Committee has

stated that the resident has received information about the camera surveillance through that he was there watching when the camera was installed, and that the boss orally explained to the resident that the purpose of the camera is to the staff should know that the resident is feeling well. It has not emerged that in addition provided some other information about the camera surveillance to the resident.

The Data Inspectorate states that the information provided by the Social Affairs Committee to the data subject (the resident) only includes information that camera surveillance is in progress, and not all the information it provides personal data controller is obliged to provide to the data subject at collection of personal data in accordance with Article 13 of the Data Protection Regulation.

The Social Affairs Committee has also stated that information has been provided to it trustee was registered. Chapter 11, Sections 4 and 7 of the Parental Code (1949: 381) state that the court may appoint a trustee for the person who, due to illness, mental disorder, impaired health or similar condition need assistance in guarding their rights, managing their property or caring for their person, and it is not enough that a good man be ordained or that the individual on any other less intrusive way gets help. The management assignment must be adapted to the needs of the individual in each particular case and may be limited to certain property or concern.

The Data Inspectorate states that even when a trustee's assignment is designed in such a way that it includes the task of caring for the individual exists there are restrictions on what a trustee is allowed to do. Of the preparatory work for the provisions on trusteeship are set out below.

In general, the principal should also be able to decide on matters himself concerning his accommodation as well as the content of the care offered. One trustees should therefore not normally represent the principal

The Data Inspectorate

DI-2019-7782

when it comes to issues of consent to, for example, surgical procedures.

Of course, this does not prevent one from e.g.

the side of care institutions obtains the administrator's views (Bill.

1987/88: 124 p 172).

The Data Inspectorate has sent a request for supplementation on 15 June 2020

requested the Social Affairs Committee to submit documentation to the Data Inspectorate regarding

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

the trustee. However, the Social Affairs Committee has not provided the information

regarding the scope of the nominee assignment and has not reported on it either

what information has been provided to the trustee. The Social Affairs Committee has in addition

nor reported its assessment that the trustee can represent it

resident regarding his right to information under Article 13 i

the Data Protection Regulation.

The Data Inspectorate's assessment

The Social Affairs Committee has not shown that there is an opportunity to provide information

the trustee, instead of the person registered in the case in question, or that it

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

The Social Affairs Committee has thus not fulfilled its duty to provide information by

inform the trustee. Nor does the information that the Social Affairs Committee has

provided to the resident is sufficient for the duty to provide information to be

fulfilled, the Social Affairs Committee's processing of personal data has also taken place in violation

with Article 13 of the Data Protection Regulation.

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

camera surveillance must be provided by clear signage or on something else effective way. It also appears that provisions on the right to information about the personal data processing such as the camera surveillance means are found in the Data Protection Ordinance and other regulations specified in section 6 KBL.

The Social Affairs Committee has not provided information that there is any sign that informs that camera surveillance is being conducted. For the Social Affairs 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 provided on something else effective way.

1 8 (22)

The Data Inspectorate

DI-2019-7782

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

The Social Affairs Committee states that it has not complied with the information requirements according to the Data Protection Regulation. The Data Inspectorate further assesses that nor did the Social Affairs Committee live up to the requirements to provide information on camera surveillance in another effective way. This means that the treatment of personal data also occurred in violation of the requirement for disclosure in § 15 KBL.

Because the resident has not received the prescribed information according to the Data Protection Ordinance and also not according to the Camera Surveillance Act can the Social Affairs Committee is not considered to have complied with the transparency requirements of Article 5 (1) (a) (i) the Data Protection Regulation.

Choice of intervention

Legal regulation

If there has been a violation of the Data Protection Regulation

The Data Inspectorate a number of corrective powers available under the article 58.2 a – j of the Data Protection Regulation. The supervisory authority can, among other things instruct the person responsible for personal data to ensure that the processing takes place in accordance with the Regulation and if required in a specific way and within a specific period.

It follows from Article 58 (2) of the Data Protection Ordinance that the Data Inspectorate in accordance with Article 83 shall impose penalty fees in addition to or in place of others corrective measures referred to in Article 58 (2), as the case may be in each individual case.

For authorities, according to Article 83 (7) of the Data Protection Regulation, national rules state that authorities may be subject to administrative penalty fees.

According to ch. 6 Section 2 of the Data Protection Act allows for penalty fees to be decided authorities, but to a maximum of SEK 5,000,000 or SEK 10,000,000 depending on whether the infringement concerns articles covered by Article 83 (4) or 83.5 of the Data Protection Regulation. Section 25 (4) KBL also states that a penalty fee can be charged by the person who conducts camera surveillance and breaks against the disclosure requirement in section 15.

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

19 (22)

The Data Inspectorate

DI-2019-7782

the seriousness of the infringement is its nature, severity and duration. About it in the case of a minor infringement, the supervisory authority may, in accordance with recital 148 i the Data Protection Regulation, issue a reprimand instead of imposing one

penalty fee.

Penalty fee

The Data Inspectorate's inspection has shown that the Social Affairs Committee has considered personal data in violation of Articles 5, 6.1, 9.2, 13, 35 and 36 of the Data Protection Regulation. In addition, the Social Affairs Committee has violated section 15 KBL.

In assessing whether the violations are so serious that an administrative sanction fee is to be imposed, the Data Inspectorate has taken into account that the processing of personal data is intended for camera surveillance of a resident of a very private sphere and in a position of dependence, where the treatment to some extent included 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 to that the Data Inspectorate has become aware of the processing through a tip from a relative of the data subject. These circumstances are seen as aggravating.

According to the Swedish Data Inspectorate's assessment, the processing did not involve one minor infringement without infringements that should lead to an administrative penalty fee.

Then the articles in the Data Protection Ordinance that the Social Affairs Committee violated covered by Article 83 (5) of the Data Protection Regulation and concerns an infringement of the duty to provide information in section 15 KBL is the maximum amount for the sanction fee in this case SEK 10 million, according to ch. Section 2, second paragraph the law (2018: 218) with supplementary provisions to the EU data protection regulation.

The administrative penalty fee shall be effective, proportionate and deterrent. This means that the amount must be determined so that it the administrative penalty fee leads to correction, that it provides a preventive effect and that it is also proportional in relation to both current

violations as to the ability of the supervised entity to pay.

In determining an amount that is efficient, proportionate and deterrent, the Data Inspectorate can state that the social committee has processed sensitive personal data about a resident in a situation that is very private and which means that housing is in a position of dependence

20 (22)

The Data Inspectorate

DI-2019-7782

towards the municipality. The violation concerns the supervision of a person in his bedroom, which is a very privacy-infringing treatment. In addition, have the treatment lasted for a relatively long time, for more than a year. The Data Inspectorate has taken into account that residents have a serious self-harming behavior, sometimes with danger to life and health both for himself and the staff.

The Social Affairs Committee has taken the measure to resolve a complex situation there staff and housing have been at risk of injury. Although the situation has been difficult to handle, the Social Affairs 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 view of the seriousness of the infringements and that the administrative the penalty fee shall be effective, proportionate and dissuasive

The Data Inspectorate that the administrative sanction fee for the Social Affairs Committee shall be set at SEK 200,000.

This decision was made by the Director General Lena Lindgren Schelin after presentation by lawyer Jeanette Bladh Gustafson. At the final

The case is also handled by the General Counsel Hans-Olof Lindblom and unit managers Malin Blixt and Charlotte Waller Dahlberg participated.

Appendix

How to pay penalty fee

Copy for information to:

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

How to appeal

If you want to appeal the decision, you must write to the Data Inspectorate. Enter i the letter which decision you are appealing and the change you are requesting.

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

2 1 (22)

The Data Inspectorate

DI-2019-7782

The Data Inspectorate forwards it to the Administrative Court in Stockholm examination.

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

2 2 (22)