Integritetsskydds myndigheten

Our Store Y AB

Prior consultation regarding analysis tools for in-store customers' movement patterns

Our Store Y AB (the company) has brought to the Swedish Authority for Privacy Protection a request for prior consultation regarding the company's planned use of an analysis tool for customers' movement patterns in the company's planned store.

The Swedish Authority for Privacy Protection submits the following opinion in response.

Summary and written advice

The Swedish Authority for Privacy Protection's advisory role includes, in accordance with Article 36 of the General Data Protection Regulation[1], providing written advice during prior consultation if the planned processing is deemed to entail a risk that personal data may be processed in violation of the law or other provision, especially if the data controller has not sufficiently established or reduced the risk.

Based on the impact assessment and the supplementary answers that the company has submitted, the Swedish Authority for Privacy Protection gives the following advice.

The Swedish Authority for Privacy Protection informs the company that, within the framework of the preliminary consultation, the authority makes no comment on whether the company's privacy-enhancing measures mean that it achieves actual anonymisation of the personal data in any part of the processing. However, the Swedish Authority for Privacy Protection states that the processing that the company is planning could be carried out with the support of Article 6.1 f of the General Data Protection Regulation on the condition that the processing of personal data only takes place for the purposes stated by the company, that the processing does not

[1] 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 the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

enable the identification of individuals, and that the other privacy-enhancing measures presented to the Swedish Authority for Privacy Protection are taken.

The authority draws the company's attention to the fact that, even if the technology is complicated, the company is obliged to provide clear and concise information to data subjects. The Swedish Authority for Privacy Protection advises the company to put up a sign, from which it is clear that the visitors' faces will be analysed and then categorised for given purposes, as well as a clear statement of the data subjects' rights, including how the data subjects can object to the processing according to Article 21 of the General Data Protection Regulation. Furthermore, the Swedish Authority for Privacy Protection advises the company to otherwise follow the guidelines for personal data processing with video devices when they need to provide information according to Article 13.

In conclusion, the authority draws the company's attention to the fact that the data controller may only hire data processors who provide sufficient guarantees that appropriate technical and organisational measures are implemented to ensure compliance with the requirements of the General Data Protection Regulation. In this regard, the Swedish Authority for Privacy Protection recommends that, to the greatest extent possible, the company settles any ambiguities regarding the distribution of responsibility for security risks between the company and the specified data processor.

Background

The company's request states, among other things, the following:

The company intends to open a store in Stockholm and then use the store's camera surveillance system to analyse its footage.

The store's cameras will send images of visitors in real time to a server located in the store. There is software installed on the server that assigns a physical visitor a so-called group ID based on their digital facial image from the store's surveillance camera as well as a time stamp linked to one of three possible time intervals for when the visitor visited the store. A group ID is a number between 1 and 1,000 used to calculate statistics on returning visitors and can be closely compared to a categorisation.
The assignment of a group ID takes place with the help of a neural network from the data processor Indivd AB. The group ID from the store's server is then sent to the data processor's cloud service, which is located in Germany, where the group ID is analysed.

The process includes several privacy-enhancing measures. The digital image from the surveillance camera used to generate a group ID is deleted after 1-

2 milliseconds. According to the company, it is practically impossible to pair a physical person who visited the store with an assigned group ID. The time stamp attached to a group ID is not an exact time but is limited to categorisation within three time intervals per day. Furthermore, the probability that a returning visitor is assigned the same group ID amounts to 50 per cent. The statistics created are thus an expression of probability.

The group ID is then sent at different time intervals to the data processor's cloud service, where the group ID is analysed in order to produce the following statistics:

1. Statistics which help in understanding how different objects in the store environment attract interest from visitors,
2. Statistics which help in understanding where and when queues form,
3. Statistics which help in understanding how visitor flows occur, and
4. Statistics which help in understanding how visitors navigate the store's planned customer route.

The analysis that the company carries out will be used to change customers' movement patterns with the aim of increasing sales and choosing places in the store where staff should be placed. In the long term, it must also be possible to compare data between different stores in order to understand differences between them.

In addition to the information about customers' movement patterns, the data processor uses information about the classification of cameras according to their location at, for example, the entrance, checkout or clothing department, time intervals used when assigning group IDs such as morning/lunch/afternoon, information about visitors that emerged during analysis of anonymised data such as total number of visits, frequency of visits, visit duration, information about objects such as shelf and product, automatic classification based on image streams of anonymous
categories of visitors' physical characteristics such as male/female and age range, aggregated anonymous data about visitors from several stores as this is collected.

The company has stated that it will carry out its processing with Article 6.1 f of the General Data Protection Regulation as the legal basis.

As the Swedish Authority for Privacy Protection understands their request, the company has stated that there are three different risks for natural persons' freedoms and rights linked to the intended processing. These risks are that the data processor's analysis tool does not mean that the personal data is anonymised and that the analysis that takes place to produce statistics can be linked to individuals, that the data subjects do not receive sufficient information and that the installation of

the data processor's analysis tool on the store's own server poses a security risk.

The Swedish Authority for Privacy Protection's advisory role

It follows from Article 36 of the General Data Protection Regulation that the person in charge of personal data must consult with the Swedish Authority for Privacy Protection before processing if a data protection impact assessment according to Article 35 shows that the processing would lead to a high risk that remains even after the person in charge of personal data has taken all measures to reduce the risk.

If the Swedish Authority for Privacy Protection finds that the planned processing would be in violation of the General Data Protection Regulation, especially if the data controller has not sufficiently determined or reduced the risk, the authority gives the data controller written advice and may use all the powers it has under Article 58 of the General Data Protection Regulation.

The Swedish Authority for Privacy Protection wishes to inform the company that this statement constitutes written advice that is not based on risks other than those that can be deduced from the documents in the case that the company submitted with their request for prior consultation. In the event that the company carries out its processing in a different way than what it has stated to the Swedish Authority for Privacy Protection, there is a risk that the advice and information provided in this statement are no longer relevant to the processing.

The Swedish Authority for Privacy Protection's opinion with written advice

Risks to data subjects' freedoms and rights

The company has stated that a certain person's assigned group ID cannot in practice be linked to the physical persons who visit the stores. At the same time, the company believes, in case it made the wrong assessment and it is possible to link the group ID to a natural person, that there is a risk that the information the company possesses might be used for extensive mapping and profiling. According to the company, such processing would lead to the processing of special categories of personal data without a legal basis, which could lead to discrimination. Furthermore, the company states that the data could be used for automated decision-making based on people's financial profiles. The company also believes that such processing involves restriction of the right to free movement and a violation of the right to privacy.

The Swedish Authority for Privacy Protection would like to inform you at the outset that, within the framework of a prior consultation, the authority cannot make a decision on whether the company processes personal data or not at a particular stage of the process. The aim of a prior consultation is

primarily for the Swedish Authority for Privacy Protection to provide advice regarding risks to the rights and freedoms of the data subjects.

The company has stated that, in practice, it is impossible to link group IDs to a single individual. According to the Swedish Authority for Privacy Protection, this indicates that the risk of linking individuals to a certain group ID is low. Furthermore, the company has stated that the analysis tool has an accuracy of 50 per cent in determining whether a visitor is a repeat visitor, which the Swedish Authority for Privacy Protection perceives as an indication that there are difficulties in using the data to map individuals because the accuracy is not high enough. Overall, the Swedish Authority for Privacy Protection finds that the risks to the rights and freedoms of data subjects that the company described in connection with the identification of individuals is to be regarded as relatively low. The Swedish Authority for Privacy Protection will therefore not provide any advice on reducing the risks that the data controller accounted for in this part.

In this context, the Swedish Authority for Privacy Protection would like to emphasise that the personal data processing that can be said to take place with certainty in the present case is the actual assignment of a group ID based on the analysis of an image of the data subject, which can most closely be compared to a categorisation of the visitors. Since the company has taken a number of privacy-enhancing measures that seem to prevent any form of analysis from being linked to individual visitors, such a categorisation could be carried out within the framework of a balance of interests according to Article 6.1 f of the General Data Protection Regulation. This is on the condition that processing of personal data only takes place for the purposes stated by the company, that the processing does not enable the identification of individuals and that the other privacy-enhancing measures presented to the Swedish Authority for Privacy Protection are taken.

In this regard, the Swedish Authority for Privacy Protection would like to add that the company's interest in the processing of personal data must be considered as relatively weak, which is why it is of great importance for the company to make a careful assessment regarding its right to process personal data in accordance with Article 6.1 f of the General Data Protection Regulation. Within the scope of the examination, the data protection officer must, among other things, examine which alternative measures can be taken to achieve the intended purpose of the processing.[2]

Information provided to the data subjects
The company has stated that it may be difficult to provide information to the data subjects that is sufficiently clear and simple. The company has stated that it will describe the processing by leaving information outside

[2] See the TK case, C-708/18 clause 49.

and inside the store, but that they will also describe the processing in their privacy policy. The company has also stated that it may be difficult to explain how the technology works.

Article 13 of the General Data Protection Regulation states what information must be provided if personal data is collected from the data subject. Article 12 states that the data controller must take appropriate measures to provide the data subject with all information referred to in Article 13, and that such information must be provided in a concise, clear, understandable and easily accessible form. Furthermore, the transparency principle in Article 5.1 a stipulates that the personal data must be processed in a legal, correct and transparent manner in relation to the data subjects.

There are no exceptions to Article 13 of the General Data Protection Regulation. However, the data controller may provide information in different layers, where a sign may constitute the first layer and information on a website or information in a brochure may constitute the second layer of information. The most important information should generally be given in the first layer.[3] The Swedish Authority for Privacy Protection also wishes to inform the company that the European Data Protection Board has adopted guidelines for processing personal data with video devices ("the guidelines"). [4]

The Swedish Authority for Privacy Protection believes that it is of great importance that the data subjects receive clear, comprehensible and accessible information before personal data processing begins. In particular, this is important as the present case concerns a new type of technology where the need to be clear in relation to the information given to the data subjects is particularly great, allowing them the opportunity to understand how their personal data will be processed by the company.

The Swedish Authority for Privacy Protection advises the company to place a sign at eye level next to the entrance to the store so that data subjects can receive the information before entering the surveilled area. On the sign, it should be clearly stated i.a. that the visitors' faces will be analysed and then categorised for given purposes, just as the sign should feature a clear statement of the rights of the data subjects, including how the data subjects can object to the processing according to Article 21 of the General Data Protection Regulation.

[3] The Article 29 Working Group (subsequently renamed EDBP), Guidelines on Transparency under Regulation (EU) 2016/679 (reviewed and adopted 11 April 2018), clause 38.

[4] See link: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices.p df

The Swedish Authority for Privacy Protection believes that, in the present case, it is of great importance that the company follows the guidelines when it makes decisions about what information should be provided and how they should provide information to data subjects.

Installation on local server
As the company's description makes clear, there is a security risk in connection with the processing of personal data. This is because a security consultant to the data processor has expressed that breaches may occur when the data processor installs its service with the data controller.[5] Furthermore, the company believes that some form of information security risk always arises when several different suppliers' systems need to be integrated and no one supplier holds overall responsibility.

The Swedish Authority for Privacy Protection notes that the company (which is stated to be the data controller) refers to an audit that the listed data processor had done. In the audit, an external consulting company points out risks linked to the data controller's security controls. The Swedish Authority for Privacy Protection believes that the company itself (which is stated to be the data controller) should reasonably assess its own security routines rather than refer to an evaluation made on behalf of the stated data processor.

The company has stated that it will take protective measures linked to password management, internet, encryption of image data, firewall routines, policies for access to the local server and penetration tests.

Furthermore, the company has stated that there is always some form of information security risk when two different suppliers collaborate and no one holds overall responsibility.

The Swedish Authority for Privacy Protection wishes to draw the company's attention to the fact that Article 28 of the General Data Protection Regulation states that if processing is to be carried out on behalf of a data controller, the data controller must only contract with data processors who provide sufficient guarantees that appropriate technical and organisational measures are implemented in such a way that the processing meets the requirements of the General Data Protection Regulation and ensure that the data subject's rights are protected. Who is the data controller and processor is determined by the actual circumstances regarding who controls the objectives and means of a processing.
The General Data Protection Regulation also allows for a shared

[5] See document 2020-3670-6.1 High level security assessment

responsibility for personal data under the circumstances mentioned in Article 26 of the General Data Protection Regulation.

Article 32 of the General Data Protection Regulation states that the data controller and the data processor must take appropriate technical and organisational measures to ensure a level of security that is appropriate in relation to the risk.

The Swedish Authority for Privacy Protection recommends that the company, as far as possible, settles any ambiguities regarding the division of responsibility regarding security risks between the company and the data processor. Furthermore, the Swedish Authority for Privacy Protection emphasises that which company constitutes the data controller for a personal data processing is determined by the actual conditions, based on the definition in Article 4 of the General Data Protection Regulation.

This opinion has been prepared by Department Manager Charlotte Waller Dahlberg after presentation by Jurist Nils Henckel. In the final processing,
Chief Legal Officer Hans-Olof Lindblom, Data Advisor Agneta Runmarker, Jurists Frida Orring, Jeanette Bladh Gustafsson, Jenny Bård and IT Security Specialist Johan Ma also participated.

Charlotte Waller Dahlberg, 2020-06-25 (This is an electronic signature)