Balance of interest / balance test for legitimate interest + Data Protection Impact Assessment

Processing operation:

The document contains a balance test for an image stream generated in conjunction with camera surveillance in stores and processed for the purpose of analyzing how people move between different geographical locations within a premise / better understanding customer flows in stores. The result should then be used to plan and customize the store layout, such as if more fitting rooms are needed.

This processing is not intended to take place separately in such a way that a camera surveillance is performed solely for the above purpose. The collected material is generated simultaneously with other image streams that are processed for other purposes, such as for security.

This document, combined with a system sketch contained in a separate document for IT and Information Security, also constitutes documentation for an data protection impact assessment according to the GDPR, Art. 35th.

1. Categories of Personal Data and Data Subjects

Category of Data Subjects	Category of Personal Data	Describe any legislative protections or whether the data otherwise could be seen as sensitive
Visitors to the areas covered by the camera surveillance at hand.	Images.	Images on humans are only biometric personal data when processed by way of technology that enables the identification or authentication of a person, for example, with facial recognition technology. In this case, the hash group key only allows a person who is a member of that group to be recognized as a member of that group.

2. Processing purposes	
To collect image material for anonymization and then analyzing anonymized and aggregated data in order to better understand customer behavior and optimize store areas. Some examples are to be able to understand how long visitors stay in the store and at different areas in the store, be able to see if there is a correlation between a certain advertising that is displayed at a certain place in the store and how many visitors who stay and/or the visitors convert / buys the product that has been displayed. There are a number of key figures for retail, developed together with the Retail Academics Research Institute Sweden AB in collaboration with Indivd AB, which demonstrate the need for analysis of how visitors move within a store / customer flows in stores with the intention to plan and adapt store layout such as if there is a need for more fitting rooms, checkouts or toilets. Other needs are to: A. adapt the utilization of resources and internal operations by predicting customer flows; B. use anonymized benchmark data to identify new cities/areas to enter C. to understand if the visitors belong to a group that have previously visited a certain area; D. reduce investment risks and become more competent traders by understanding how changes in the store environment affect conversion rates and re-visit rates; E. increase the transfer of knowledge across the organization by sharing insights in a web-based platform and F. adapting business models, such as introducing a yoga studio or a running club in a sporting goods store or adapting rent depending on the attractiveness of the surface.	
3. Legal basis/bases for the processing	
Legitimate interests under Article 6 (1) (f) in GDPR.	
Where legitimate interests are relied on as a legal basis, do the GDPR, ePrivacy Regulation or any other regulation specifically identify the processing activity as being legitimate?	No.

4. Legitimate interests - balancing test	
4.1 Balancing test questions	
Question	**Answer/comments**
Is the processing in the interests of the data subjects?	Data subjects will ultimately get a better store experience when visiting the store in question.
In whose interests is the processing taking place and why are they important?	To our knowledge, stores currently lack the ability to efficiently collect and analyze information about their visitors in order to produce statistics and be able to customize / plan their operations. There are examples of stores that try to understand the behavior of their visitors by appointing staff who manually review / monitor visitors and take notes. Such a method assumes that the person conducting the survey / monitoring the visitors actually observes the same. In our view, this arrangement creates a greater risk of visitors' personal integrity being violated as they are actually observed compared to an automatic / non-manual analysis of anonymized data. In addition, the current method will lead to great inefficienciency, lead times in inventory management, irrelevant advertising, inefficient planning and use of surface, inefficient reception and other similar waste of resources in the retail sector. Effective and appropriate data analysis has great potential for increased margins and cost reductions in the pressed retail industry.
What would the impact be if you couldn't go ahead with the processing?	Reduced efficiency and greater integrity infringement through current manual methods that require observation. Continued waste of resources in retail, the retail apocalypse and continued very large and increasing difficulties in competing with e-commerce.
If you have received information from a third party, have the data subjects been informed that the information would also be used by third parties (such as you) for the intended purposes?	Not applicable.
Could individuals whose personal data it relates to be negatively impacted by the processing? If so, what is the likelihood and the severity of any such impact?	No. Our opinion is that the result benefits the individuals. The risk of negative impact on data subjects is small, given the extensive technical and organizational security measures, including, in particular that the analyses are made on anonymized group data. Image data is transferred to a processing instance operated by Indivd, where it is anonymized and deleted within milliseconds. Personal data is processed but never stored. Only anonymous statistical data is retained. The risk of personal data breaches has

	been managed through extensive technical and organizational security measures. These are described in a separate document.
Would individuals reasonably expect or anticipate that the processing activities take place, or that their information is used for the connected purposes?	Information is provided in an appropriate privacy notice for the camera surveillance.
Are the Data Subjects scored and/or evaluated? E.g. with regard to performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements.	No.
Does the processing involve elements of automated decision making?	No, not in relation to the data subjects.
Does the processing prevent Data Subjects from exercising a right or using a service or a contract?	No.
Is your intended purpose and method widely understood?	No.
Would you be happy to explain the processing to individuals?	Yes.
Are some people likely to object to the processing or find it intrusive?	The solution is technically complex and easy to misunderstand, but our assessment is that objections are unlikely if the people in question understand the solution.
Are you processing personal data of vulnerable Data Subjects? Such as (i) employees (ii) children (iii) vulnerable segments of the population, e.g. the mentally ill, asylum seekers, or the elderly, a patient, or in any case where there is an imbalance in the relationship between the position of the Data Subjects and the Controller.	Yes, but the purpose of the processing is not intended to be adapted accordingly. Information that causes sensitive data to be processed is abundant information and is deleted within 1-2 milliseconds after anonymization has taken place.
How will you prevent function creep?	With high protection class. See description of security measures in separate document. The data in the current image stream is deleted within 1-2 milliseconds after anonymization has taken place.
Does the processing mean that Data Subjects are systematically monitored?	Yes, but only 1-2 milliseconds, until deletion.
Is the processing conducted on a large scale? Taking into account: a. the number of Data Subjects concerned, either as a specific number or as a proportion of the relevant population; b. the volume of data and/or the range of different data items;	There are currently no fixed limits for what is considered to be a large-scale processing, but we deem that that it may qualify as large-scale processing, despite it being limited in time.

c. the duration, or permanence; and d. the geographical extent.	
Do the data originate from two or more data processing operations performed for different purposes and/or by different controllers? If so, would the Data Subjects expect these data to be combined?	No.
4.2. Assessment of the necessity and proportionality of the Processing operation in relation to the purpose	
4.2.1 Confirmation of adherence to General Processing Principles	**Comments**
The intended Data Processing Activity is appropriate to achieve the processing purposes and the legitimate interests	Yes, the alternative is manual observational studies. The proposed method is less privacy violating than manual observational studies.
There are no less intrusive Data Processing Activities that would also achieve the processing purposes and the legitimate interests	Not to our knowledge. There are methods to calculate the number of visitors, but these do not provide the same information but are limited to a pure calculation exercise for how many people who visit the store. There are also services that track people in the store, but these require that the store's wi-fi or a web application is used and consent is given, or that a web application is provided. In our opinion, these solutions are more privacy intrusive. They also require visitor activity, which makes the data less accurate as far from all visitors will choose to connect to the wi-fi or web application in question.
The intended Data Processing Activity is necessary to achieve the processing purposes and the legitimate interests	Yes, there are no satisfactory alternative solutions for the retail industry today.
The intended Data Processing Activity is adequate because the interests of the responsible legal entity outweigh the interests of the Data Subjects	Yes.
The intended Data Processing Activity is adequate because the Personal Data is limited to what is necessary to achieve the processing purposes and the legitimate interests (minimization)	Yes.
The access to the Personal Data affected by the intended Data Processing Activity is limited to those individuals with a need to Process the Personal Data to achieve the processing purposes and the legitimate interests	No person has access to the personal data. The images have a high degree of protection. See description of security measures in separate document.
4.2.2 Measures contributing to the proportionality and necessity of the Processing on the following bases	

Personal Data shall be collected for specific, explicit, and legitimate purpose(s) and is not further Processed in a manner that is incompatible with those purposes ("purpose limitation"): The personal data may only be used to assign an ID based on facial features in order to avoid that an individual is assigned to more than one group, each group containing 50 visitors, and to calculate hash group keys per group of 50 visitors. A grouping which is conducted with approximately 50% accuracy,
Processing is lawful (in accordance with the legitimate interests): That is our understanding.
Personal Data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are Processed ("data minimization"): The personal data/raw data is automatically deleted after 1–2 milliseconds in Indivd's Anonymizer, which operates via a secure VPN tunnel to the customer's location from Indivd's cloud environment.
Safeguards to reduce/mitigate any underlying privacy risks or harms: Described in separate document.
4.2.3 Measures contributing to the rights of the Data Subjects
Proper information is provided to the Data Subjects and the Data Subjects have been consulted: Visitors are informed through the store's privacy policy. They are however not consulted.
Right of access and portability: The personal data processed is in images that are provided on request.
Right to rectify, erase, object, restriction of Processing: Images can be requested according to customary routines to manage the rights of registered persons. The anonymized data cannot be linked to individuals and therefore do not constitute personal data.
Recipients: The data is shared with a supplier who manages the operation of our server and environment.
Processor: Indivd AB for possible support of the software Indivd Anonymizer (see information in the IT and Information Security document).
Safeguards surrounding international transfer(s): Not applicable.
Consultations of experts: The document has been prepared with the support of Indivd AB.
Other comments: