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

Description of processing activity

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.

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. Similarily, data blurred with noise only allows a person to be identified as a probabilistic distribution of several individuals and with no way to be identified or singled out based on this data.
2. Purpose of the processing

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 for the processing

Legitimate interests, 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**
4.1.1 Is the processing in the interests of the individuals?	Individuals will ultimately get a better store experience when visiting the store in question.
4.1.2 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.
4.1.3 What would the impact be if you could not carry out 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.
4.1.4 If you have received information from a third party, have the individuals been informed that the information would also be used by third parties (such as you) for the intended purpose(s)?	Not applicable.

4.1.5 What is the intended effect on the individuals? Can the processing affect the individuals negatively? If so, what is the likelihood of such negative effects and how serious are they?	No. Our opinion is that the result benefits the individuals provided that correct analyses are made and that correct conclusions are drawn from the data used for the statistics. The risk of negative impact on individuals is small, given the extensive technical and organizational security measures, including, in particular that the analyses are made on anonymized data. Processing of personal data takes place locally in the customer's environment, where the personal data is anonymized. The data transferred to Indivd's environment does not constitute personal data. It is this data that is used as a basis for producing statistics. The risk of personal data breaches has been managed through extensive technical and organizational security measures. These are described in a separate document.
4.1.6 Would individuals reasonably expect and foresee that the processing is done, or that their personal data are used for the intended purposes?	Yes, as information is provided in an appropriate privacy notice for the camera surveillance.
4.1.7 Are the individuals 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.
4.1.8 Does the processing comprise automatic decision-making?	No, not in relation to the individuals.
4.1.9 Does the processing involve innovative use or application of new technological or organizational solutions? What is the current state of technology in this area?	Yes. Other companies that provide people counting solutions are based on camera surveillance that seem to have a less robust solution in terms of of anonymization.
4.1.10 Are there any current issues of public concern that should be factored in? If so, describe these.	No, there are no current issues of public concern that should be factored in.
4.1.11 Does the processing hinder the individuals from exercising a right or to use a service or an agreement?individual	No.
4.1.12 Are the intended purpose and method commonly known?	No.
4.1.13 Would you be comfortable with explaining the processing for the individuals?	Yes.
4.1.14 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.

4.1.15 Is there an imbalance in power between the individuals and the controller?	No.
4.1.16 Are you processing personal data of vulnerable individuals? Such as (iii) 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 individuals 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.
4.1.17 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.
4.1.18 How will you ensure data quality and data minimization?	[Data quality is ensured by Quality Assurance by the supplier] Personal data is immediately deleted (cf. below)
4.1.19 Is the personal data shared with anyone? If so, please describe the nature of the receivers (including whether these act as joint controllers, independent controllers or data processors) and the purpose(s) of such sharing and any agreements regulating the sharing.	It is shared with our supplier,Indivd AB, acting as processor. The processing is regulated in the data processing agreement.
4.1.20 Does the processing mean that individuals are systematically monitored?	Yes, but only 1-2 milliseconds, until deletion.
4.1.21 Is the processing conducted on a large scale? Taking into account: a. the number of individuals 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 being processed; c. the duration, or permanence, of the data processing activity; d. the geographical extent of the processing activity.	There are currently no fixed limits for what is considered to be a large-scale processing, but we think that it is likely that the camera surveillance would qualify as large-scale processing.
4.1.22 Do the personal data originate from two or more processing activities that are being performed for different purposes and/or by different controllers? Where this is the case, would the individuals reasonably expect that the data sets were combined and processed for the intended purpose(s)?	No.

4.2. Assessment of whether the processing is necessary and proportionate in relation to its purpose	
4.2.1 Confirmation of compliance with fundamental principles of the GDPR	**Comments**
4.2.1.1 The intended processing is appropriate to achieve its purpose(s) and legitimate interests.	Yes, the alternative is manual observational studies. The proposed method is less privacy violating than manual observational studies.
4.2.1.2 There are no less intrusive processing activities that may lead to fulfilment of the purposes and satisfaction of 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.
4.2.1.3 The intended processing is necessary to achieve the purpose(s) and the legitimate interests.	Yes, there are no satisfactory alternative solutions for the retail industry today.
4.2.1.4 The intended processing is appropriate since the controller's interests override the interest(s) of the individuals of not having their personal data processed for the intended processing purpose(s).	Yes.
4.2.1.5 The intended processing is appropriate since the personal data is limited to what is necessary to achieve the purpose(s) of the processing and the legitimate interests (minimization).	Yes.
4.2.1.6 The access to the personal data is limited to the individuals that need to process the personal data to achieve the processing purpose(s) 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	

4.2.2.1 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 either generate a blurred embedding or 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 is conducted with approximately 50% accuracy. Any noisy embedding is sufficient noisy to be at least equivalent in data protection to k-anonymity with k = 3.
4.2.2.2 Processing is lawful (in accordance with the legitimate interests): Yes, that is our understanding.
4.2.2.3 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 processing 1-2 milliseconds in Indivds Anonymizer. Additional data transmission times from camera to data processing server are kept to a minimum, which amounts to a few seconds or minutes and during which the data is both strongly encrypted and inaccessible.
4.2.2.4 Safeguards to reduce/mitigate any underlying privacy risks or harms: Described in separate document.
4.2.3 Measures contributing to the rights of the individuals
4.2.3.1 What is the nature of your relationship with the individuals? Describe how/if information is provided to the individuals and whether their views have been sought. Relationship is that the individuals are visitors to the store. They are informed through the store's privacy policy, but not consulted.
4.2.3.2. Describe whether the right of access and data portability are supported. Right of access: right of access could be handled, but it would be limited in practice due to the short retention time. Right to data portability: N/A. This right applies where consent or contractual necessity serves as a legal basis for the processing activity.
4.2.3.3 Describe whether the right to rectification and erasure are supported. Right to rectification: We do not see how right to rectification should come into play for this processing activity. Right to erasure: unlikely to apply in practice, given the short retention time.

4.2.3.4 Describe whether the right to objection and restriction of processing are supported. Right to objection: unlikely to apply in practice, given the short retention time. Right to restriction of processing: unlikely to apply in practice, given the short retention time.
5. Technical and organizational security measures
5.1 Pseudonymization (as result, personal data cannot be attributed to a specific individual without the use of additional information and this additional information is kept separately from the personal data): N/A, we anonymize.
5.2 Encryption in storage and/or in transit: Yes. See Data Processing Agreement.
5.3 Access controls: Yes. See Data Processing Agreement.
5.4 Access logging: Yes. See Data Processing Agreement.
5.5 Logging of changes: Yes. See Data Processing Agreement.
5.6 Routines to continuously backup the personal data: No, the personal data is automatically deleted.
5.7 Other safeguards: Yes. See Data Processing Agreement.
5.8 Describe whether third country transfers take place. If so, describe the safeguards that apply and whether a transfer impact assessment has been conducted. No third-country transfers take place.
6. Consultation of experts

Consultations of experts: The document has been prepared with the support of Indivd AB.
Other comments: