Indivd demographic classification add-on: Balance of interest / balance test for legitimate interest + Data Protection Impact Assessment under the GDPR, Art. 35

Background and description of processing activity:

This document, relating to demographic classification should be read together with the document *People Counter: Balance of interest / balance test for legitimate interest + Data Protection Impact Assessment* and *People Counter data – Quality Assurance: Balance of interest / balance test for legitimate interest + Data Protection Impact Assessment under the GDPR, Art. 35.* The processing activity covered in the first mentioned document is hereinafter referred to as the "**Main processing activity**".

Customers wishing to refine the outcome of the Main processing activity may order the demographic classification add-on. This add-on is thus provided as an ancillary service to the People Counter services. The demographic categories are intentionally broad, further enhancing the privacy of the individuals. Examples of categories include:

- Age Group
- Perceived Gender Expression
- Style (e.g., business professional, comfortable, colorful, urban/street)
- Clothing Features (e.g., presence of coat or hat)

The system does not classify based on protected characteristics such as race, ethnicity, religion, or any biometric identifier.

Per Art. 35 of the GDPR, a data protection impact assessment ("DPIA") shall be carried out *where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.*

On the basis of how the demographic classification service is designed and provided, we do not deem that the associated processing of personal data qualifies as high risk, rendering a DPIA mandatory. Diligent controllers may however still decide to carry out a DPIA.

In light of the foregoing and in the interest of transparency and comfort to our customers, acting as controllers, Indivd AB, acting as a processor in providing the demographic classification services, has prepared this document. Customers may use it as part of their documentation of a legitimate interest balance test (LIA) or a DPIA.

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.	No. Images of individuals are only considered biometric personal data (cf. Article 4(14) GDPR) when processed by means of technology that enables the unique identification or authentication of a person, for example, through facial recognition. In this case, the classification is based on a coarse demographic estimation (such as perceived age group or gender expression), performed within milliseconds in volatile memory, and the result is assigned to a transient Group Anonymity Token. The data is not used to identify or track any individual, nor is it retained in a form that would allow such identification. The processing is therefore not considered to involve special categories of personal data as defined in Article 9 GDPR, including biometric data. .

2. Purposes of the processing

In order to ensure that the processing purposes for the Main processing activity are achieved at a refined demographic level. Demographic classification fulfils such purpose.

In other words, image material is collected and anonymized on an aggregated level in order to better understand the composition and behavior of visitors at a population level.

Some examples are to be able to identify which demographic groups (such as approximate age group or perceived gender expression) are more likely to visit certain areas within the store, to evaluate which product zones attract specific segments, and to support changes in store layout or marketing strategy based on statistical trends in visitor demographics.

Other processing purposes:

A. adapt the utilization of resources and internal operations by predicting demographic flow patterns;
B. use anonymized benchmark data to compare demographic engagement across stores or regions;
C. understand how different demographic groups respond to changes in campaigns, assortment, or layout;
D. reduce investment risks and increase strategic precision by analyzing behavior and representation across various demographic groups;
E. adapt business models, such as introducing new services, product lines, or concepts, based on the demographic composition of store visitors.

3. Legal basis for the processing	
Legitimate interests under Article 6 (1) (f) in GDPR.	
Where the legal basis for the processing is legitimate interest, Art. 6 (1)(f) of the GDPR, do the GDPR, ePrivacy Directive or any other applicable law state that the type of processing is lawful?	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?	Yes. Just like for the Main processing activity, 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, physical stores currently lack the ability to efficiently collect and analyze demographic information about their visitors in order to produce anonymized statistics to customize and plan their operations. There are examples of stores that try to understand the composition of their visitors by appointing staff to manually observe and note demographic features. Such methods assume that the person conducting the observation can do so consistently and objectively, which often leads to subjective results and creates a greater risk to visitors' personal integrity, as they are directly observed. Other existing methods, such as Wi-Fi/Bluetooth tracking or third-party profiling, do not offer direct demographic insight and involve the processing of personal data with a higher risk to privacy.

	In comparison, Indivd's demographic classification enables anonymous demographic analysis in a scalable and privacy-preserving way. Processing is done in-memory, no identifiers are created, and only aggregated statistical data is retained. This significantly reduces the privacy risks to data subjects and replaces more intrusive legacy methods with a data protection-by-design approach.
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, limited understanding of visitor composition, and increasing challenges in responding to demographic shifts and consumer behavior. For the Main processing activity: without the ability to generate anonymized insights, stores would continue relying on high-risk or inaccurate alternatives, such as manual surveys, third-party profiling, or device tracking — all of which either lack precision or pose significant data protection concerns. Demographic classification is a privacy-preserving refinement of the Main processing activity.
4.1.4 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.
4.1.5 What is the intended effect on individuals? Can the processing affect the individuals negatively? If so, what is the likelihood of such negative effects and how serious are they?	The intended effect is an improved visitor experience. No negative effects on the individuals, in our opinion. 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 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 and used as a basis for producing statistical demographic insights. The risk of personal data breaches has been managed through extensive technical and organizational security measures. These are described in a separate document (Demographic classification - How it works - 2025-10-26).
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. Information is provided in an appropriate privacy notice for the camera surveillance.
4.1.7 Are the individuals evaluated or scored? E.g. regarding performance at work, financial situation, health, personal preferences or interests, reliability or behavior, geographic position or movement.	No.
4.1.8 Does the processing involve elements of automated 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?	In our opinion, the Main processing activity is innovative. For this ancillary demographic classification, we are also not aware of any other company in this line of business (people counting) that uses this type of demographic classification.
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?	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 well enough.
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 (i) employees; (ii) children; (iii) vulnerable individuals, such as mentally ill, asylum seeking individuals, elderly, patients or other individuals where there is an imbalance in power between 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 limiting access to the data. See description of security measures in separate document (Section Sections 10 and 11, Demographic classification - How it works - 2025-10-26). In addition, it should be emphasized that 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?	The demographic classification in itself is not recurring nor extended in time (1-2 milliseconds) and the classifications are intentionally broad.
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 processor, Indivd AB, that carries out the demographic classification. The processing is regulated in the data processing agreement.
4.1.20 Does the processing entail systematic monitoring of the individuals	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 deem that that it may qualify as large-scale processing, despite it being limited in time.
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 the necessity and proportionality of the Processing operation in relation to the purpose	
4.2.1 Confirmation of adherence to General Processing Principles	**Comments**
4.2.1.1 The intended processing is appropriate to achieve its purpose(s) and legitimate interests.	Yes, just like for the Main processing activity: 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 purpose(s) and satisfaction of the legitimate interests	Not to our knowledge. There are methods to calculate the number of visitors, but these do not provide demographic information and are limited to a pure calculation of how many people visit the store. Other methods used in the industry—such as manual observation, Wi-Fi or Bluetooth tracking, third-party data aggregation, or biometric computer vision—either lack the ability to generate reliable, real-time demographic insights or involve significantly higher privacy risks. Wi-Fi and Bluetooth tracking collect persistent device identifiers and still require additional data to estimate demographics. Third-party profiling relies on inferred and often outdated data collected without transparency or valid consent. Facial recognition systems provide granular data but introduce high privacy risks and require the processing of biometric personal data. By contrast, Indivd's demographic classification performs real-time anonymization in volatile memory and outputs only aggregated statistics. The system does not generate or retain identifiers, and no personal data is stored. In our opinion, this solution is less privacy intrusive and efficient than existing alternatives while achieving the intended purpose.

4.2.1.3 The intended processing is necessary to achieve the purpose(s) and the legitimate interests.	Yes, to our knowledge, 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 (Section Sections 10 and 11, Demographic classification - How it works - 2025-10-26).
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 assign an ID based on facial features in order to ensure that an individual is not assigned to more than one group, each group containing approximately 50 visitors, and to calculate hash group keys per group. This grouping is conducted with approximately 50% accuracy and solely for the purpose of enabling anonymous demographic statistics at population level.	
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 1–2 milliseconds in Indivd’s Anonymizer, which operates via a secure VPN tunnel to the customer's location from Indivd’s cloud environment.	
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 concerned individuals and whether their views have been sought. The relationship is that that the individuals are visitors to the store. They are informed through the store's privacy policy. They are, however, 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. Personal data is automatically deleted after completed demographic classification.
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.
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.

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. See e.g. Section 2 in Demographic classification - How it works - 2025-10-26. *The module extends anonymized statistics by linking each Group Anonymity Token to a limited set of perceived demographic categories, while ensuring that no personal data remain after the anonymization stage. All processing follows the principles of data minimization, storage limitation, and data protection by design, in line with Articles 5 and 25 GDPR.*

5.2 Encryption in storage and/or in transit: Yes. See Section 11 in Demographic classification - How it works - 2025-10-26 and Data Processing Agreement.

5.3 Access controls: Yes. See Section 11 in Demographic classification - How it works - 2025-10-26 and Data Processing Agreement

5.4 Access logging: Yes. See Section 11 in Demographic classification - How it works - 2025-10-26 and Data Processing Agreement

5.5 Logging of changes: Yes. See Section 11 in Demographic classification - How it works - 2025-10-26 and Data Processing Agreement

5.6 Routines to continuously backup the personal data: No. Personal data is automatically deleted within 1-2 milliseconds after the demographic classification has been completed.

5.7 Other safeguards: Yes. See Section 11 in Demographic classification - How it works - 2025-10-26 and 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

The document has been prepared with the support of Indivd AB.

7. Risk assessment
7.1 **Risks**: Please describe the various risks associated with the processing operation, risk sources, threats that could lead to unlawful access and the potential impact of the risk to the rights and freedoms of the individuals concerned. Also, describe whether the risk is deemed to be unlikely, potential, likely or highly likely We deem that the risks relating to potential impact of the risk to the rights and freedoms of the individuals concerned are low. For supporting documentation on risks related to technical and organizational measures, Demographic classification - How it works - 2025-10-26.
7.2 **Severity**: Please appreciate the severity level of the identified risk, based on three severity levels; low, medium or high Low
7.3 **Measure(s):** How do you envisage that the identified risks shall be handled? We deem that the risks have been appropriately handled.
7.4 **Result**: Is the risk eliminated, reduced or accepted? We deem that the risk is acceptable.
7.5 **Evaluation**: Is the final impact on the individuals after implementing the proposed solution a justified, compliant and proportionate response to the aims of the project? Are there still high residual risks, meaning that a prior consultation should be sought with the supervisory authority. We deem that the residual risks are not at a level that merit a prior consultation with the supervisory authority.