Indivd Drop-in Rate feature: 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 the Drop-in Rate feature, should be read together with the document People Counter: Balance of interest / balance test for legitimate interest + Data Protection Impact Assessment under the GDPR, Art. 35. The processing activity covered in that document is hereinafter referred to as the "Main processing activity".

Customers wishing to measure the conversion efficiency of their physical storefronts may order the Drop-in Rate feature. This feature is provided as an ancillary service to the People Counter services. It combines two independent anonymous counts: the number of people passing in front of a store window (passers-by stream) and the number of people entering the store (entrance stream). The ratio of these two counts constitutes the Drop-in Rate. Neither stream uses re-identification, biometric processing, or any form of demographic inference. No image is retained. The output is a single anonymous ratio, such as: for every hundred people who walked past, how many entered.

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. Where this is the case, Art. 35 (3) (c) further states that a DPIA shall in particular be required in the case of systematic monitoring of publicly accessible places on a large scale.
On the basis of how the Drop-in Rate feature is designed and provided, including the applied anonymization, it can be argued that the associated processing of personal data qualifies as high risk, rendering a DPIA mandatory.

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 the context of the Drop-in Rate feature, has prepared this document. Customers may use it as part of their documentation of a legitimate interest balance test (LIA) or a DPIA, but are encouraged to seek its own legal advice, as needed.

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, including pedestrians passing in front of the store window and individuals entering the store.	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 processing is limited to detecting whether a human-shaped object has crossed a virtual counting line. No facial geometry is analysed, no demographic attribute is inferred, no biometric template is created, and no individual identifier is assigned or retained. The data is not used to identify or track any individual. 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

Image material is collected and anonymised on an aggregated level in order to understand the conversion efficiency of physical storefronts and window displays at a population level. The Drop-in Rate metric measures what proportion of individuals passing in front of a store window or display, within the camera's field of view, actually enter the store.

Some examples are to evaluate whether a window display or store location is attracting a sufficient share of available pedestrian traffic; to measure the effect of changes in window merchandising, signage, or promotional content on storefront conversion; and to compare Drop-in Rate performance across a retailer's store network.

Other processing purposes:

A. adapt the utilisation of resources and internal operations by predicting pedestrian flow patterns and storefront conversion trends;
B. use anonymised benchmark data to compare Drop-in Rate performance across stores or regions;
C. understand how changes in store presentation, location, or external environment affect conversion rates;
D. reduce investment risks and increase strategic precision in store location and window display decisions;
E. adapt business models, such as adjusting opening hours, staffing levels, or window refresh frequency, based on observed pedestrian conversion patterns.

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?	The processing takes place in the interests of retailers, commercial property operators, shopping centre operators, and airport operators who need to understand the conversion efficiency of their physical storefronts and window displays. To our knowledge, physical stores currently lack the ability to continuously and accurately measure what proportion of pedestrians passing their storefront actually enter the store. Without this metric, retailers cannot distinguish between low conversion caused by poor location and low conversion caused by an ineffective window display, limiting their ability to make evidence-based decisions on merchandising investment, lease renewal, and store layout. Existing methods for measuring audience engagement at storefronts typically involve significantly higher privacy risk. Camera-based audience measurement systems commonly used in the market process facial geometry to infer gaze direction, attention duration, and demographic attributes such as age and gender. These systems require facial analysis and produce individual-level inferences, placing them in substantially more contested legal territory under GDPR. Mobile device signal collection relies

	on persistent device identifiers that constitute personal data under GDPR. Manual observation by staff constitutes direct observation of individuals in a public space. Infrared beam sensors count entrants only and cannot produce a Drop-in Rate because the passers-by denominator is absent. In comparison, Indivd's Drop-in Rate feature detects only the presence of a human-shaped object crossing a virtual line. No face is analysed, no demographic attribute is inferred, no identifier is created, and no image is retained. Only anonymous aggregate counts are produced. This is the least privacy-intrusive method currently available for producing the Drop-in Rate metric continuously at scale, and represents a materially lower privacy risk than the camera-based alternatives commonly deployed in the market.
4.1.3 What would the impact be if you could not carry out the processing?	Without the Drop-in Rate feature, retailers would have no scalable, privacy-preserving method to measure storefront conversion continuously. They would be forced to rely on one of the following alternatives: manual observation by staff, which is directly privacy-intrusive, episodic, and not scalable across a multi-site network; mobile device signal collection, which carries materially higher regulatory risk under GDPR; or camera-based systems that require facial geometry analysis, which involve more contested legal territory than anonymous body-presence counting. The commercial consequence is that retailers cannot distinguish between low conversion caused by poor location and low conversion caused by an ineffective window display. This limits evidence-based decision-making on window merchandising investment, lease renewal, store layout, and promotional effectiveness, resulting in continued waste of resources and reduced ability to compete with digital commerce.
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 store environment for visitors as a result of better-informed retail decisions on window displays, store layout, and location investment. No negative effects on individuals, in our opinion. No decision is made about any individual as a result of the processing. The output is an anonymous aggregate ratio that describes population-level behaviour only. The risk of negative impact on data subjects is minimal, given that no image is retained, no identifier is created, no demographic attribute is inferred, and no individual can be singled out from the output. Image data is transferred to a processing instance operated by Indivd, where it is anonymised and deleted within 1-2 milliseconds. Indivd AB operates the processing as a data processor under a data processing agreement. Personal data is processed but never stored. Only anonymous statistical data is retained and used as a basis for producing the Drop-in Rate statistic. The risk of personal data breaches has been managed through extensive technical and organisational security measures. These are described in a separate document (Drop-in Rate - How it works - 2026-03-30).
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?	No.

E.g. regarding performance at work, financial situation, health, personal preferences or interests, reliability or behavior, geographic position or movement.	
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 Drop-in Rate feature, we are not aware of any other company in this line of business (people counting) that produces a continuous Drop-in Rate metric using camera-based anonymous body-presence counting with immediate on-device image deletion and no biometric processing.
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?	No person has access to the personal data. The images have a high degree of protection. See description of security measures in Sections 9 and 10 in Drop-in Rate - How it works - 2026-03-30.
4.1.18 How will you ensure data quality and data minimization?	The counting operation is not recurring nor extended in time at the individual level (1-2 milliseconds). The output is a single integer count increment with no individual attributes. No information beyond body presence is processed.
4.1.19 Is the personal data shared with anyone?	It is shared with our processor, Indivd AB, that operates the Drop-in Rate counting feature. The processing is regulated in the data processing agreement.

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.	
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. Infrared beam sensors count entrants only and cannot produce a Drop-in Rate because the passers-by denominator is absent. Manual observation can produce the required metric but requires staff stationed outside the store, is not scalable, is subject to human error, and constitutes direct observation of individuals in a public space. Mobile device signal collection relies on persistent device identifiers that constitute personal data under GDPR and carries materially higher regulatory risk. Camera-based audience measurement systems commonly used in the market process facial geometry to infer gaze direction, attention duration, and demographic attributes, placing them in more contested legal territory under GDPR than pure body-presence counting. By contrast, Indivd's Drop-in Rate feature processes image frames in volatile memory, deletes them within 1-2 milliseconds, extracts only a binary detection result, and retains only anonymous aggregate counts. No identifiers are generated or retained, and no personal data is stored beyond the detection

	instant. In our opinion, this is the least privacy-intrusive method currently available for producing the Drop-in Rate metric continuously at scale.
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.
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 detect whether a human-shaped object has crossed a defined virtual counting line, for the sole purpose of incrementing an anonymous counter. No facial features, demographic attributes, or any other individual characteristics are extracted or retained. The only persistent output is an anonymous integer count.	
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 minimisation"): The personal data/raw data is automatically deleted within 1-2 milliseconds after the presence detection operation completes. No image, biometric data, or individual attribute is retained at any stage. The only persistent output is an anonymous integer counter value.	
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 The relationship is that the individuals are either visitors to the store or pedestrians on a public street. They are informed through the store's privacy notice and, for the outdoor passers-by camera, through visible signage at the monitored location in accordance with EDPB Guidelines 3/2019. 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 extremely short retention time. Personal data is automatically deleted within 1-2 milliseconds after detection. 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 extremely short retention time of 1-2 milliseconds. Personal data is automatically deleted immediately after detection. The anonymised data cannot be linked to individuals and therefore does 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 Drop-in Rate - How it works - 2026-03-30. Each image frame is processed to produce a binary detection result and immediately deleted. No Group Anonymity Token, no demographic category, and no individual attribute is created. 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 Sections 9 and 10 in Drop-in Rate - How it works - 2026-03-30 and Data Processing Agreement.
5.3 Access controls: Yes. See Sections 9 and 10 in Drop-in Rate - How it works - 2026-03-30 and Data Processing Agreement.
5.4 Access logging: Yes. See Sections 9 and 10 in Drop-in Rate - How it works - 2026-03-30 and Data Processing Agreement.
5.5 Logging of changes: Yes. See Sections 9 and 10 in Drop-in Rate - How it works - 2026-03-30 and Data Processing Agreement.
5.6 Routines to continuously backup the personal data: No. Personal data is automatically deleted within 1-2 milliseconds after detection. No backup of personal data is created.
5.7 Other safeguards: Yes. See Sections 9 and 10 in Drop-in Rate - How it works - 2026-03-30 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 organisational measures, cf. Drop-in Rate - How it works - 2026-03-30 and the Data Processing Agreement.
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.