

People Counter data – Quality Assurance: Balance of interest / balance test for legitimate interest + Data Protection Impact Assessment ("DPIA") under the GDPR, Art. 35

Background and description of processing activity:

This document, relating to Quality Assurance of People Counter data should be read together with the document *People Counter: Balance of interest / balance test for legitimate interest + Data Protection Impact Assessment*. The processing activity covered therein is hereinafter referred to as the "**Main processing activity**".

In order to ensure that the processing purposes for the Main processing activity are achieved, the data quality needs to be ensured. Quality Assurance services are thus provided as an ancillary service to the People Counter services for customers who seek comfort and a way to demonstrate data quality.

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 Quality Assurance services are designed and provided, we do not deem that the associated processing of personal data qualifies as high risk, rendering a DPIA mandatory. The Swedish Authority for Privacy Protection ("**the IMY**") does however recommend on its website¹ that DPIA's are carried out for borderline cases.

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 Quality Assurance services, has prepared this document for its Quality Assurance services. Customers may use it as part of their documentation of a legitimate interest balance test (LIA) or a DPIA.

¹ Last updated 8 September 2021, checked 17 November 2023, only available in Swedish here:
<https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/konsekvensbedomningar-och-forhandssamrad/>

1. Categories of Personal Data and categories of Data Subjects

Categories of Data Subjects	Categories of Personal Data	Are there specific regulations under law that cover the type of intended processing? Are the personal data considered sensitive?
Visitors to the areas covered by the camera surveillance at hand.	Images	No.

2. Purpose of the processing

In order to ensure that the processing purposes for the Main processing activity are achieved, the data quality needs to be ensured. Quality Assurance services fulfil such purpose.

3. Legal basis for the processing

Legitimate interests, Art. 6.1 (f) of the 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 interest – balancing test

4.1 Balancing test questions

Question	Answer/comments
4.1.1 Is the processing in the <u>interest of the individuals</u> ?	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 <u>whose interests</u> is the processing taking place and why are they important?	Physical 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. In order to ensure that the processing purposes for the Main processing activity are achieved, the data quality needs to be ensured. Quality Assurance services serves to fulfil such purpose.
4.1.3 What would the <u>impact be if you could not carry out</u> the processing?	The Main processing activity could risk being questioned as not being reliable enough.

4.1.4 If you have received information from a third party, have the individuals been <u>informed that the information would also be used by third parties</u> (such as you) for the intended purpose(s)?	Not applicable.
4.1.5 What is the <u>intended effect on individuals</u> ? 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.
4.1.6 Would individuals <u>reasonably expect and foresee</u> that the processing is done, or that their personal data are used for the intended purposes?	Yes. Quality assurance as such should not be unexpected and information is provided in an appropriate privacy notice for the camera surveillance.
4.1.7 Are the individuals <u>evaluated or scored</u> ? 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 comprise <u>automatic decision-making</u> ?	No, not in relation to the individuals.
4.1.9 Does the processing involve <u>innovative use or application of new technological or organizational solutions</u> ? What is the <u>current state of technology</u> in this area?	In our opinion, the Main processing activity is innovative. For this ancillary Quality Assurance, we understand that similar technologies are used for quality assurance purposes, such as in the automotive industry. We are however not aware of any other company in this line of business (people counting) that uses this type of quality assurance.
4.1.10 Are there any current <u>issues of public concern</u> 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 <u>hinder the individuals from exercising a right or to use a service or an agreement</u> ?	No, the processing does not hinder the individuals from exercising a right or to use a service or an agreement.
4.1.12 Are the intended <u>purpose and method commonly known</u> ?	The intended <i>purpose</i> (quality assurance) is commonly known. As for the <i>method</i> , we understand that similar technologies are used for quality assurance purposes, such as in the automotive industry. We are however not aware of any other company in this line of business (people counting) that uses this type of quality assurance.
4.1.13 Would you be <u>comfortable with explaining</u> the processing for the individuals?	Yes.
4.1.14 Is it <u>likely that some individuals would object to the processing or find it intrusive</u> ?	No.

4.1.15 Is there an <u>imbalance in power</u> between the individuals and the controller?	No.
4.1.16 Does the processing comprise <u>vulnerable individuals</u> ? 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 not used in the Quality Assurance.
4.1.17 How will you <u>prevent function creep</u> ?	The supplier only uses well trained staff to carry out the Quality Assurance and technical and organizational measures have been implemented to ensure that only such individuals can access the personal data.
4.1.18 How will you ensure <u>data quality and data minimization</u> ?	The purpose of the processing itself is to ensure data quality. The Quality Assurance is not recurring nor extended in time, but limited to an isolated technical verification of the installed equipment. The typical data collection period is one hour. Personal data is not stored following completed Quality Assurance, i.e. following one manual observation. The Quality Assurance is completed within 48 hours from the data collection.
4.1.19 Is the personal data <u>shared</u> 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 Quality Assurance. The processing is regulated in the data processing agreement.
4.1.20 Does the processing entail <u>systematic monitoring</u> of the individuals?	Yes, we deem that this may qualify as systematic monitoring, however without being privacy intrusive. The Quality Assurance is not recurring nor extended in time, but limited to an isolated technical verification of the installed equipment. The typical data collection period is one hour.
4.1.21 Is the processing conducted on a <u>large scale</u> ? 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 it is unlikely that the camera surveillance would qualify as large-scale processing, as this is limited in time and to an isolated technical verification/Quality Assurance of the installed equipment.
4.1.22 Do the personal data <u>originate from two or more processing activities</u> that are being performed for different purposes and/or by different controllers?	No.

Where this is the case, would the individuals <u>reasonably expect that the data sets were combined</u> and processed for the intended purpose(s)?	
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 <u>appropriate</u> 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 <u>no less intrusive processing activities</u> that may lead to fulfilment of the purpose(s) and satisfaction of the legitimate interests.	Not to our knowledge. We also deem that manual quality assurance (that would be the option) would be less accurate.
4.2.1.3 The intended processing is <u>necessary</u> to achieve the purpose(s) and the legitimate interests.	Yes.
4.2.1.4 The intended processing is <u>appropriate</u> 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 (<u>minimization</u>).	Yes.
4.2.1.6 The <u>access to the personal data is limited</u> to the individuals that need to process the personal data to achieve the processing purpose(s) and the legitimate interests.	Yes.
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 supplier only uses well trained staff to carry out the Quality Assurance and technical and organizational measures have been implemented to ensure that only such individuals can access the personal data.	
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 deleted directly after the Quality Assurance has been completed, i.e. after one manual observer has viewed the data once.	

4.2.2.4 Safeguards to reduce/mitigate any underlying privacy risks or harms: See Section 4-5 in How it works document, Security Assessment documentation, Data Processing Agreement.
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. Relationship is that 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 <u>right of access and data portability</u> 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 Quality Assurance, i.e. after one manual observer has viewed the data once. 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 <u>right to rectification and erasure</u> 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 <u>right to objection and restriction of processing</u> 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 3.6 in the How it works document <i>The manual observers try to discern whether the two people are the same. If so, the flow count is increased by one. We do not store the classification and the image pairs, afterwards the image is terminated.</i>
5.2 Encryption in storage and/or in transit: Yes. See Section 4-5 How it works document and Data Processing Agreement.
5.3 Access controls: Yes. See Section 4-5 How it works document and Data Processing Agreement.
5.4 Access logging: Yes. See Section 4-5 How it works document and Data Processing Agreement.
5.5 Logging of changes: Yes. See Section 4-5 How it works document and Data Processing Agreement.
5.6 Routines to continuously backup the personal data: No, the personal data is automatically deleted after one manual observer has viewed the data once.
5.7 Other safeguards: Yes. See Section 4-5 in How it works document, Security Assessment documentation, 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
<p>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</p> <p>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, cf. the Security Assessment documentation.</p>
<p>7.2 Severity: Please appreciate the severity level of the identified risk, based on three severity levels; low, medium or high</p> <p>Low</p>
<p>7.3 Measure(s): How do you envisage that the identified risks shall be handled?</p> <p>We deem that the risks have been appropriately handled.</p>
<p>7.4 Result: Is the risk eliminated, reduced or accepted?</p> <p>We deem that the risk is acceptable.</p>
<p>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.</p> <p>We deem that the residual risks are not at a level that merit a prior consultation with the supervisory authority.</p>

Appendix 1 Systematic description of the processing

The assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels):

Schedule/flow chart: See How it works document.