Approved by
December 18, 2018
Order No. 1-2.1/125

Datu valsts inspekcija

Data State Inspectorate of the Republic of Latvia

Blaumaņa iela 11/13-15, Rīga, LV-1011, Latvia, phone +371 67223131, fax +371 67223556, e-mail info@dvi.gov.lv, www.dvi.gov.lv

in Riga

**List of processing operations
requiring data protection impact assessment
pursuant to Article 35 (4) of the GDPR**

Data State Inspectorate of the Republic of Latvia (hereinafter – the Inspectorate) in accordance with Article 35 (3) and 35 (4) of the General Data Protection Regulation (GDPR) has developed list of the kind of processing operations which is the subject to the requirement for a data protection impact assessment (hereafter – the List).

The List is based on Working Party 29 Guidelines WP248 on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 of 4th October, 2017 (Guidelines). The List complements and specifies the Guidelines. in accordance with the following criteria deriving from the Guidelines (hereafter – the Criteria):

1. Evaluation or scoring, including profiling and predicting, especially from "aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements" (recitals 71 and 91).

Example - a financial institution that screens its customers against a credit reference database or against an anti-money laundering and counter-terrorist financing (AML/CTF) or fraud database, or a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company building behavioural or marketing profiles based on usage or navigation on its website.

2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person" (Article 35(3)(a)).

Example - the processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion.

3. Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks or "a systematic monitoring of a publicly accessible area" (Article 35(3)(c)) 15.

Example - this type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s).

4. Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10.

Example - general hospital keeping patients' medical records or a private investigator keeping offenders' details. Beyond these provisions of the GDPR, some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals.

5. Data processed on a large scale: the GDPR does not define what constitutes large scale, though Recital 91 provides some guidance. In any event, the WP29 recommends that the following factors, in particular - be considered when determining whether the processing is carried out on a large scale:
    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 being processed;
c. the duration, or permanence, of the data processing activity;
d. the geographical extent of the processing activity.

6. Matching or combining datasets.

Example - originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.

7. Data concerning vulnerable data subjects (recital 75);

Example - children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data), employees, more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, etc.), and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.

8. Innovative use or applying new technological or organizational solutions, like combining use of finger print and face recognition for improved physical access control, etc.

Example - certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy; and therefore, require a DPIA.

9. When the processing in itself "prevents data subjects from exercising a right or using a service or a contract" (Article 22 and Recital 91).

Example - bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

The Inspectorate indicates that the List cannot be considered exhaustive.

The Controller before the processing must take into account the nature, scope, context and purposes of the processing in all cases, and the likelihood of the processing to result in a high risk to the rights and freedoms of natural persons in the spirit of Article 35 (1) GDPR and prepare a data protection impact assessment where the Controller considers that the processing may result in a high risk to freedoms and rights of natural persons.

Considering the mentioned above, Controllers, whose main or only place of establishment is the territory of the Republic of Latvia, will be required to conduct the data protection impact assessment on the processing of data at least in following cases:

1) processing of personal data relating to criminal convictions and offences or related security measures.
2) processing of personal data for scientific or historical purpose without the consent of the data subject when in conjunction with at least one of the Criteria.
3) When the provision of information referred to in Article 19 to data subject proves impossible.
4) Processing of genetic data for the purpose to uniquely identifying a natural person when in conjunction with at least one of the Criteria.
5) Surveillance carried out in at least one of the following cases:
    a. When carried out on a large scale;
    b. When carried out at workplace;
    c. When directed at vulnerable data subjects (for example, in health care, social care, imprisonment institutions, prisons, educational institutions, work place).
6) Regarding data processing through the use of innovative technologies, mechanisms or new procedures when in conjunction with at least one of the Criteria.
7) Processing of personal data involving measures for systematic monitoring of employee activities.
8) Large scale tracking of data subjects, including lifestyle apps or logistic companies.
9) Use of location data regarding a data subject, when in conjunction with at least one other Criteria mentioned above is applicable.
10) Data processing when information society services are offered directly to a child.
11) Large scale automatic personal data processing and processing based on profiling.
12) Where the purpose of data processing is to combine data from various sources for matching, comparison and re-use purposes.
13) Biometric data processing for the purpose to uniquely identifying a natural person, when in conjunction with at least one other Criteria mentioned above.

Kind regards
Data State Inspectorate of Latvia