REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

List of cross-border processing operations which are subject to the requirement for a data protection impact assessment

In case of cross-border data processing (see GDPR art. 35 (6)), the aspect of large scale processing shall not be defined by exact minimum number of data subjects. Therefore, the data controllers needs to adhere to the following requirements when conducting cross-border personal data processing.

The following list is indicative and given examples complement and further specify the requirement set out in Art 35(1) of the GDPR and the criteria listed in the WP248 *"Guidelines 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"*.

Data protection impact assessment needs to be done by every data controller, when taking into account the nature, scope, context and purposes of the processing there is the likely outcome of a high risk to a natural person.

The GDPR (art 35 (3)) provides three examples of this.

1. The first example is about profiling - the data controller/processor evaluates natural persons:
    a. by using automated processing
    b. extensively (large scale)
    c. systematically and
    d. this kind of evaluation produces legal effects to concerning natural person or significantly affects the natural person.
2. The second example is about processing special categories of data or data about criminal convictions on a large scale.
3. The third example is about systematic monitoring of a publicly accessible area on a large scale.

Based on the WP243 and WP248 Guidelines, following factors should 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.

Examples listed in Art 35(3) of the GDPR are not exhaustive. Therefore, other kind of personal data processing, that might pose a high risk comparable to the previous three examples, also need the data protection impact assessment. For instance:

4. Processing of biometric data for the purpose of uniquely identifying a natural person, on a large scale.
5. Processing of genetic data, on a large scale.
6. Processing in the context of employment that involve systematic monitoring of employees activities, on a large scale.

Large scale processing, that:

7. Might pose a risk of identity theft or fraud (particularly in digital trust services and in comparable identity management services).
8. Might pose a risk of property loss (particularly in banking and credit card services).
9. Might pose a risk of violation of secrecy of correspondence (particularly in communication services).
10. Involve tracking of location in real time (particularly in communication services).
11. Might pose a risk of disclosure of personal economical stand (particularly taxation data, banking data, credit ranking data – publicly available data is not taken into account).
12. Might pose a risk of discrimination with legal consequences or with similar impact (particularly in labor broking services and in assessment/evaluation services having impact on salaries and career).
13. Might pose a risk of loss of statutory confidentiality of information (restricted information, professional secrecy).

We emphasize that previously mentioned lists and examples are not exhaustive, as examples in GDPR art 35 (3) itself are not exhaustive.