REPUBLIC OF CROATIA
PERSONAL DATA
PROTECTION AGENCY

Zagreb, 13 December 2018

LIST OF THE TYPES OF PROCESSING FOR WHICH A DPIA SHALL BE REQUIRED PURSUANT TO ARTICLE 35.4 GDPR

Having regard to the EDPB Opinion 25/2018 on the draft list of the competent supervisory authority of Croatia regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR),

Based on Art. 35.4 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (General Data Protection Regulation, *hereinafter:* GDPR),

Based on the Working Party 29 Guidelines on Data Protection Impact Assessment (WP 248),

the Director of the Croatian Personal Data Protection Agency adopts the following decision:

The impact assessment of the protection of personal data is compulsory in the processing of personal data in the following cases:

1) Processing personal data for systematic and extensive profiling or automated decision-making to bring conclusions that are of significant influence or may affect an individual and / or several persons or that help to decide about someone's access to a service (or service) or convenience (e.g. such as personal data processing related to economic or financial status, health, personal preferences, interests, reliability, behavior, location data, and other)

2) Processing special categories of personal data for profiling or automated decision making

3) Processing of personal data of children for profiling or automated decision making or for marketing purposes, or for direct offering of services intended for them;

4) Processing of personal data collected from third parties that are considered for making decisions regarding the conclusion, termination, rejection or extension of service contracts to natural persons;

5) Processing of special categories of personal data or personal data on criminal or misdemeanor liability in a large extent;

6) Processing of personal data by using systematic monitoring of publicly available places in large scale;

7) Use of new technologies or technological solutions for personal data processing or possibility of personal data processing (e.g. application of "internet of things" such as smart TVs, smart home appliances, communicated toys, smart cities, smart energy meters etc..) that serve to analyze or predict the economic situation, health, personal preferences or interests, reliability or behavior, location or movement of natural persons;
8) Processing of biometric data in combination with any of the other criteria set out in WP29 DPIA Guidelines;
9) Processing of genetic data in combination with any of the other criteria set out in WP29 DPIA Guidelines;
10) Personal data processing by linking, comparing or verifying multi-source matching;
11) Processing of personal data in a manner that involves monitoring the location or behavior of an individual in the case of systematic processing of communication data (metadata) generated by the use of the telephone, the Internet or other communication channels such as GSM, GPS, Wi Fi, monitoring or processing of location data;
12) Personal data processing using devices and technologies in which an incident may endanger the health of an individual or more individuals;
13) Processing personal information of employees using applications or monitoring systems (e.g. processing of personal data for monitoring of work, movement, communication, etc.).

In addition, the Personal Data Protection Agency emphasizes that the existence of a list of the type of processing for which DPIA shall be required, does not in any way diminish the general obligation of the data controller to carry out an appropriate risk assessment and risk management. Also, the enforcement of the impact assessment on data protection does not relieve data controllers of the obligation to comply with other obligations of the GDPR or other obligations contained in the applicable legislative framework (EU or national).

Furthermore, the said list is in no case limited or exhaustive, since the performance assessment of the effect on the protection of data is always necessary if the conditions of Article 35.1 of the GDPR are met. In addition to this, the Personal Data Protection Agency also points to the fact that the list is subject to further development and may be changed in accordance with the additional observed or incurred processing risks.

Therefore, the data controller for one of the abovementioned processing types is required to evaluate the effect on data protection before processing.

However, this does not necessarily mean the obligation to carry out the prior consultation. If the risk can be adequately reduced by appropriate technical and organizational measures, then no prior consultation is necessary.