
**List of the types of processing operations for which a DPIA shall be required (Section 35 (4) of the GDPR)**

Each supervisory authority has the obligation to establish a list of the types of processing operations for which a DPIA shall be required, in accordance with Article 35 (4) of the GDPR. Such draft list was prepared by the Belgian Commission for the Protection of Privacy and has been confirmed by the Belgian Data Protection Authority on June 13th 2018. The Belgian Authority communicated this list to the European Data Protection Board (EDPB) for its opinion in accordance with Article 64 of the GDPR.

The Board shared its view in its opinion 2/2018 of September 25th 2018. The Authority adapted its draft taking into account the recommendations formulated by the Board and officially adopted its list on 16th January 2019.

As a reminder, where this list concerns processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union, the consistency mechanism referred to in article 63 shall be applied prior to the development of the list.[1]

The Authority emphasizes that the existence of a list of processing operations for which it is mandatory to carry out a DPIA in no way undermines the general obligation of the controller to carry out proper risk assessment and risk management. Carrying out a DPIA also does not exempt the controller from the obligation to comply with other obligations of the GDPR or other obligations imposed by general or sector-specific legislation. Moreover, the list below is by no means exhaustive: carrying a DPIA is always required as soon as the conditions of application defined in article 35 (1) of the GDPR have been met.[2] In addition, the Authority would like to draw attention to the *Guidelines on Data Protection Impact*

[1] Article 35 (6) of the GDPR.

[2] The mere fact that a data processing does not correspond to one of the types of the listed processing (for example, because one of the characteristics is not present) does not mean that there would be an exemption for this processing from the obligation to carry out a DPIA in accordance with Article 35 (1) of the GDPR.

*Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (EU) 2016 /* 679 adopted by the Article 29 Working Party on April 4th 2017 and last revised and adopted on October 4th 2017, which constitute an essential element of the list established by the Authority since these guidelines provide a common base to ensure consistency within the Union, whereby each national list complements and further clarifies these guidelines. Finally, the Authority also draws attention to the fact that these lists are evolving and can be adapted if they fail to achieve their intended objective

In addition to the cases provided for in section 35 (3) of the GDPR and taking into account the exception provided for in article 35 (10) of the GDPR, carrying out a DPIA shall be compulsory in the following cases:

1. when the processing makes use of biometric data[3] for the purpose of uniquely identifying data subjects who are in a public space or in a private publicly accessible area;
2. when personal data are collected from third parties and subsequently taken in to account in the context of a decision to refuse or terminate a specific service contract with a natural person;
3. when health data of a data subject are collected by automated means with the aid of an active implantable medical device[4];
4. when data are collected on a large scale from third parties in order to analyze or predict the economic situation, health, personal preferences or interests, reliability or behaviour, location or movements of natural persons;
5. when special categories of personal data within the meaning of Article 9 of the GDPR[5] or data of a very personal nature (such as data on poverty, unemployment, involvement of youth care or social work, data on household and private activities, location data) are systematically exchanged between several controllers;
6. in case of a large-scale processing of data generated by means of devices with sensor that send data via the Internet or via other means ("Internet of Things" applications, such as smart televisions, smart household appliances, connected toys, "smart cities", smart energy meters, etc.) that serves

[3] Article 4 (14) of the GDPR defines "biometric data" as being personal data resulting from a specific technical processing, relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

[4] It concerns any active medical device that is designed to be implanted wholly or partly in the human body or in a natural orifice and is intended to remain after the intervention.

[5] Special categories of data according to Article 9 includes in particular personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

to analyze or predict the economic situation, health, personal preferences or interests, reliability or behavior, location or movements of natural persons;

7. in case of large-scale and/or systematic processing of telephony, Internet or other communication data, metadata or location data of natural persons which allows to trace natural persons (for example, Wi-Fi tracking or processing of location data of passengers in public transport) when the processing is not strictly necessary for a service requested by the data subject;

8. in case of large-scale processing of personal data whereby the behavior[6] of natural persons is systematically observed, collected, established or influenced by automated processing, including for advertising purposes.

The controller who envisages one of the aforementioned types of processing is obliged to carry out a DPIA prior to the processing. However, this does not necessarily mean that prior consultation must also take place. If the risk can be adequately reduced with the implementation of appropriate technical and organizational measures, no prior consultation shall be required.

[6] For example viewing, listening, browsing, clicking, physical or purchasing behaviour.