



LIST OF THE TYPES OF DATA PROCESSING THAT
REQUIRE A DATA PROTECTION IMPACT ASSESSMENT
UNDER ART 35.4

Data Protection Impact Assessments (hereinafter DPIA) are regulated under Section 3 of Chapter IV ('Data controller and data processor') of General Regulation (EU) 2016/679 on Data Protection of the European Parliament and of the Council of 27 April (hereinafter GDPR).

Specifically, article 35 (1) establishes in general terms the duty incumbent on data-processing controllers to carry out a DPIA prior to the commencement of any processing where it is likely that the nature, scope, context, or purposes of the said processing poses a high risk to the rights and freedoms of natural persons, which high risk, according to the Regulations themselves, will be increased where the processing is carried out using 'new technologies'.

In addition, article 35.3 provides that a DPIA shall be specifically required in the following circumstances:

- a) a systematic and extensive evaluation of personal aspects relating to natural persons based on automated processing, such as profiling, where this forms the basis for decisions giving rise to legal effects concerning the natural person or has a significant similar effect on the natural person;
- b) processing on a large scale of special categories of data referred to in article 9 (1), or of personal data relating to criminal convictions and offences referred to in article 10, or
- c) the systematic monitoring of a publicly accessible area on a large scale.

In order to assist controllers in identifying the kinds of data-processing that require a DPIA, the GDPR provides that supervisory authorities must publish a list setting out what kind of processing requires a DPIA. This list shall be notified to the European Data Protection Board (EDPB).

OUTLINE LIST OF THE TYPES OF DATA PROCESSING THAT REQUIRE A DATA PROTECTION IMPACT ASSESSMENT UNDER ARTICLE 35.4 GDPR

When it comes to examining real data-processing situations, where the said processing meets two or more of the criteria listed below, it will be necessary to carry out a DPIA in the majority of cases, unless the processing falls within the list of processing that does not require a DPIA under article 35.5 of the GDPR. The more criteria that the processing in question meets, the greater the risk that the said processing entails, and the greater the certainty that it requires a DPIA.

This list, based on the criteria established by the Article 29 Working Party in guide WP248, ‘Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of the GDPR’, complements them and should be understood to be a non-exhaustive list.

1. Processing that involves profiling or the evaluation of subjects, including the collection of the subject’s data in multiple areas of his/her life (work performance, personality, and behaviour), covering various aspects of his/her personality or habits.
2. Processing that involves automated decision-making or that makes a significant contribution to such decision-making, including any kind of decision that prevents data subjects from exercising a right or accessing a product or service or forming part of a contract.
3. Processing that involves the observation, monitoring, supervision, geo-location, or control of the interested party in a systematic and extensive manner, including the collection of data and metadata via networks, applications, or in publicly accessible areas, as well as the processing of unique identifiers that allow the identification of users of services of the information society, such as web services, interactive TV, mobile applications, etc.
4. Processing that involves the use of special categories of data as referred to in article 9.1 of the GDPR; data concerning criminal convictions and offences as referred to in article 10 of the GDPR, or data that allow the financial situation or solvency to be determined, or that allow personal information in relation to special categories of data to be determined or deduced.
5. Processing that involves the use of biometric data for the purpose of uniquely identifying a natural person.

6. Processing that involves the use of genetic data for any purpose.
7. Processing that involves the use of data on a large scale. In order to determine whether processing can be considered to be on a large scale, the criteria laid down in guide WP243, ‘Guidelines on Data Protection Officers (DPOs)’ of the Article 29 Working Party shall be taken into account.
8. Processing that involves the association, combination, or linking of records in databases from two or more data-processing events with different aims or by different controllers.
9. Data processing regarding vulnerable subjects or those who are at risk of social exclusion, including the data of persons aged under 14, older people with any kind of disability, the disabled, persons who access social services, and the victims of gender-related violence, as well as their descendants and persons who are in their guardianship or custody.
10. Processing that involves the use of new technologies or an innovative use of consolidated technologies, including the use of technologies on a new scale, for a new purpose, or in combination with others, in a manner that entails new forms of data collection and usage that represents a risk to people’s rights and freedoms.
11. Data processing that prevents interested parties from exercising their rights, using a service, or executing a contract, such as for example processing where data have been compiled by a controller distinct from the controller who is to process them, and any of the exceptions regarding the information that ought to be provided to the interested parties under article 14.5 (b,c,d) of the GDPR apply.