HELLENIC DATA PROTECTION AUTHORITY

Athens, 16-10-2018
Protocol Number: Γ/ΕΞ/8189/16-10-2018

List of the kind of processing operations which are subject to the requirement for a data protection impact assessment according to article 35 par. 4 of GDPR

Legal basis

According to article 35 par. 4 of GDPR, the supervisory authority establishes and makes public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment (DPIA) pursuant to par. 1 and communicates this list to the European Data Protection Board (EDPB).

Where this list involves 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.

Background

A DPIA is required when a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons (article 35 par. 1 of GDPR). Conducting a DPIA is required in particular in the cases referred to in article 35 par. 3 of GDPR.

In order to provide a more concrete set of processing operations for which a DPIA is required due to their inherent high risk, the Article 29 Working Party has adopted the guidelines entitled "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" (WP248 rev.01). The above guidelines set out nine criteria that data controllers should use to determine whether or not a DPIA has to be carried out.

Definition of large scale

When determining whether the processing is carried out on a large scale, it is recommended that the following factors, in particular, be considered on the basis of the DPIA guidelines (WP248) as well as the guidelines entitled "Guidelines on Data Protection Officers ('DPOs')" (WP243):

a. the number of data subjects involved, either as a specific number or as a percentage of the relevant population;

b. the volume of data and / or the range of data items being processed;

c. the duration or the permanent nature of the data processing activity;

d. the geographical scope of the processing activity.

Kind of processing operations which are subject to DPIA

The present list groups and further specifies the kind of processing operations for which DPIA is required including indicative examples. This list is not exhaustive and does not remove or alter the obligation to conduct a DPIA in all cases where the conditions of article 35 par.1 of GDPR are met. This list is based on article 35 of GDPR and in particular par. 1 and 3 as well as the Working Party 29 guidelines on DPIA (WP248), which it complements and further specifies.

The criteria for carrying out a DPIA are grouped in the following three categories:

- *1st category:* based on the types and purposes of the processing.
- *2nd category:* based on the types of personal data and/or categories of data subjects.
- *3rd category:* based on the additional characteristics and/or means of the processing.

Conducting a DPIA shall be compulsory when at least one of the criteria of the 1st or the 2nd category is met. It shall also be compulsory when at least one of the criteria of the 3rd category is met and the processing concerns types and purposes of the 1st category, and/or types of personal data and/or categories of data subjects of the 2nd category.

1st category: types and purposes of the processing

1.1 Systematic evaluation, scoring, prediction, prognosis and profiling, especially of aspects concerning the data subject's economic situation, health, personal preferences or interests, reliability or behaviour, location or movements or the credit rating of data subjects.
Indicative examples include the case in which a financial institution screens its customers on the basis of credit reference data or anti-money laundering and counter-terrorist financing or fraud data, or the case in which a biotechnology company offers genetic tests directly to consumers in order to assess and predict the disease/health risks.

1.2 Systematic processing of personal data that aims at taking automated decisions producing legal effects concerning data subjects or similarly significantly affects data subjects and may lead to the exclusion or discrimination against individuals.
Indicative examples are the automatic refusal of an online credit application or e-recruiting practices without any human intervention (recital 71 of GDPR) or an automatic refusal of insurance provision.

1.3 Systematic processing of personal data which may prevent the data subject from exercising its rights or using a service or a contract, especially when data collected by third parties are taken into account.
Indicative examples are the case where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan or not, registering the data subject in a "black" list, such as the list of mobile operators or registering the data subject in whistleblowing systems.

1.4 Systematic processing of personal data concerning profiling for marketing purposes when the data are combined with data collected from third parties.

1.5 Large scale systematic processing for monitoring, observing or controlling natural persons using data collected through video surveillance systems or through networks or by any other means over a public area, publicly accessible area or private area accessible to an unlimited number of persons. It includes the monitoring of movements or location/geographical position on real time or not real time of identified or identifiable natural persons.
Indicative example are the use of video surveillance cameras in shopping malls/centers or public transportation stations, or the processing of location data of passengers in the airport or in public transportation. Also, the wi-fi tracking of visitors in shopping centers or the processing of personal data using drones.

1.6 Large scale systematic processing of personal data concerning health and public health for public interest purposes as is the introduction and use of electronic prescription systems and the introduction and use of electronic health records or electronic health cards.

1.7 Large scale systematic processing of personal data with the purpose of introducing, organizing, providing and monitoring the use of electronic government services, as defined in article 3 of L.3979/2011 as applicable.

2nd category: types of personal data and/or categories of data subjects.

2.1 Large scale processing of special categories of personal data referred to in Article 9 par. 1 (including genetic data and biometric data for the purpose of uniquely identifying a natural person) and of personal data referred to in Article 10 of GDPR.

2.2 Large scale systematic processing of data of high significance or of a highly personal nature as are
- 2.2.1 Data of social welfare (data concerning poverty, unemployment, social work etc.),
- 2.2.2 Data of electronic communications, including the content of the communications such as electronic mail, metadata and data of geographic position/location, with the exception of telephone call recording pursuant to art.4 par.3 of L.3471/2006,
- 2.2.3 Data concerning the national identity number or other identifiers of general application or the alteration of the conditions and terms of processing and use of them and of other related to them personal data,
- 2.2.4 Data included in personal documents, diaries, notes from e-readers and in life-logging applications equipped with note-taking features and very personal information,
- 2.2.5 Data collected or generated by means of devices (such as these with sensors) especially through the 'internet of things – IoT' applications (such as smart televisions, smart household appliances, connected toys, smart cities, smart energy meters etc.) and/or by using other means.

2.1 Systematic monitoring – provided that it is fair – of the position/location of employees as well as of the content and of the metadata of employee communications with the exception of logging files for security reasons provided that the processing is limited to the absolutely necessary data and is specifically documented. A relative example that falls into the obligation of carrying out a DPIA is the use of DLP systems.
Processing of biometric data for the purpose of uniquely identifying a natural person as well as genetic data of employees.

3rd category: additional characteristics and/or means of the processing.

3.1 Innovative use or application of new technological or organizational solutions, which can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms, like the combined use of fingerprint and face recognition for improved physical access control, or mhealth applications, or other "smart" applications from which user profiles are generated (e.g. daily habits), or artificial intelligence applications as well as publicly accessible blockchains that include personal data.

3.2 Matching and/or combining personal data originating from multiple sources or third parties, or for 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 subjects.

3.3 In case the processing concerns personal data that has not been obtained from the data subject and the information to be provided to data subjects pursuant to Article 14 of GDPR proves impossible or would require a disproportionate effort or is likely to render impossible or seriously impair the objectives of the processing.

Revision

The above list is subject to regular revisions every two years or to an unscheduled revision due to significant developments in technology or in operational models, as well as in the case of a change in the purposes of the processing when these new purposes present high risk.