

Opinion of the Board (Art. 64)



Opinion 22/2018

on the draft list of the competent supervisory authority of the United Kingdom

regarding

the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)

Adopted on 25th September 2018

Contents

| | |
|--|---|
| 1. Summary of the Facts | 4 |
| 2. Assessment | 5 |
| 2.1 General reasoning of the EDPB regarding the submitted list | 5 |
| 2.2 Application of the consistency mechanism to the draft list | 6 |
| 2.3 Analysis of the draft list..... | 6 |
| Reference to the Guidelines | 6 |
| Biometric data..... | 6 |
| Genetic data..... | 6 |
| Location data | 7 |
| Data collected via third parties (article 19 GDPR) | 7 |
| Exceptions to information to be provided to the data subject according to article 14.5 GDPR | 7 |
| Employee Monitoring | 8 |
| Processing using new/innovative technology | 8 |
| 3. Conclusions / Recommendations | 8 |
| 4. Final Remarks..... | 9 |

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU 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 (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter “DPIA”). They shall, however, apply the consistency mechanism where such lists involve processing operations, 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.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is “likely to result in a high risk to the rights and freedoms of natural

persons”. Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Information Commissioner’s Office (hereafter Supervisory Authority of the United Kingdom) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 9th of July 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Supervisory Authority of the United Kingdom shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Supervisory Authority of the United Kingdom, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Supervisory Authority of the United Kingdom to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which

criteria have been taken into account by the Supervisory Authority of the United Kingdom to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Supervisory Authority of the United Kingdom relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Supervisory Authority of the United Kingdom does not contain such a statement, the Board recommends the Supervisory Authority of the United Kingdom to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Supervisory Authority of the United Kingdom for an opinion of the Board states, that the processing of biometric data falls under the obligation to perform a DPIA on its own. The Board is of the opinion that the processing of biometric data on its own is not necessarily likely to represent a high risk. However, the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Supervisory Authority of the United Kingdom to amend its list accordingly, by adding that the item referencing the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

GENETIC DATA

The list submitted by the Supervisory Authority of the United Kingdom for an opinion of the Board states, that the processing of genetic data falls under the obligation to perform a DPIA

on its own. The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Supervisory Authority of the United Kingdom to amend its list accordingly, by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

LOCATION DATA

The Board is of the opinion that the processing of location data on its own is not necessarily likely to represent a high risk. However, the processing of location data in conjunction with at least one other criterion requires a DPIA to be carried out. The list submitted by the Supervisory Authority of the United Kingdom for an opinion of the Board does currently require a DPIA to be carried out when there is a processing of location data on its own. The Board requests the Supervisory Authority of the United Kingdom to amend its list accordingly, by adding that the item referencing the processing of location data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

DATA COLLECTED VIA THIRD PARTIES (ARTICLE 19 GDPR)

The Board is of the opinion that types of processing activities that could deprive the data subjects from their rights in conjunction with at least one other criterion represent a high risk. Further, the Board is of the opinion that a processing activity conducted by the controller under article 19 GDPR and where the information of recipients would prove impossible or require a disproportionate effort only requires a DPIA to be carried out when this processing involves at least one other criterion. The list submitted by the Supervisory Authority of the United Kingdom for an opinion of the Board states that this type of processing in conjunction with at least one other criterion falls under the obligation to perform a DPIA. The Board takes note of the inclusion of this criterion in the list.

EXCEPTIONS TO INFORMATION TO BE PROVIDED TO THE DATA SUBJECT ACCORDING TO ARTICLE 14.5 GDPR

The Board is of the opinion that types of processing activities that could deprive the data subjects from their rights do not represent a high risk on their own. Therefore, a processing activity conducted by the controller under article 14 GDPR and where the information to be given to the data subjects is subject to an exemption under article 14.5 (b)-(d) could require a DPIA to be carried out only in conjunction with at least one other criterion. The list submitted by the Supervisory Authority of the United Kingdom for an opinion of the Board does currently require a DPIA to be done for the processing of data where article 14(5), para (b), (c) and (d) applies on its own. The Board requests the Supervisory Authority of the United Kingdom to amend its list accordingly, by adding that it requires a DPIA only in conjunction with at least one other criterion.

EMPLOYEE MONITORING

The Board is of the opinion that, due to its specific nature, the employee monitoring processing, meeting the criterion of vulnerable data subjects and of systematic monitoring in the guidelines, – could require a DPIA. Given that the list submitted by the Supervisory Authority of the United Kingdom for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment, the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

PROCESSING USING NEW/INNOVATIVE TECHNOLOGY

The list submitted by the Supervisory Authority of the United Kingdom for an opinion of the Board envisages that the use of new or innovative technology, on its own, requires a DPIA. The Board is of the opinion that the use of innovative technology on its own is not necessarily likely to represent a high risk. However, the use of innovative technology in conjunction with at least one other criterion requires a DPIA to be carried out. Therefore, the Board requests the Supervisory Authority of the United Kingdom to amend its list accordingly, firstly by referring in their list to innovative technology and secondly by adding that the item requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

3. Conclusions / Recommendations

The draft list of the Supervisory Authority of the United Kingdom may lead to an inconsistent application of the requirement for a DPIA and the following changes need to be made:

- Regarding the reference to the guidelines: the Board requests the Supervisory Authority of the United Kingdom to amend its document accordingly.
- Regarding biometric data: the Board requests the Supervisory Authority of the United Kingdom to amend its list by adding that the item referencing the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding genetic data: the Board requests the Supervisory Authority of the United Kingdom to amend its list by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding location data: the Board requests the Supervisory Authority of the United Kingdom to amend its list by adding that the item referencing the processing of location data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding the exceptions to the information to be given to the data subjects according to article 14.5 GDPR: the Board requests the Supervisory Authority of the United Kingdom to amend its list by adding that it requires a DPIA only in conjunction with at least one other criterion.

- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.
- Regarding processing using new or innovative technology: the Board requests the Supervisory Authority of the United Kingdom to amend its list firstly by referring in their list to innovative technology and secondly by adding that the item requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

4. Final Remarks

This opinion is addressed to the Information Commissioner's Office (Supervisory Authority of the United Kingdom) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)