

Recommendations



**Recommendation 01/2019 on the draft list of the European
Data Protection Supervisor regarding the processing
operations subject to the requirement of a data protection
impact assessment
(Article 39.4 of Regulation (EU) 2018/1725)**

Adopted on 10 July 2019

Table of contents

- 1 SUMMARY OF THE FACTS..... 4
- 2 ASSESSMENT 4
 - 2.1 General reasoning of the EDPB regarding the submitted list 4
 - 2.2 Analysis of the draft list..... 5
- 3 CONCLUSION 7

The European Data Protection Board

Having regard to Article 70(1)(e) 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 Article 39(4) of Regulation (EU) 2018/1725 EU of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (hereinafter Regulation 2018/1725),

Having regard to Article 12 and Article 22 of its Rules of Procedure of 25 May 2018, as revised on 23 November 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereinafter GDPR) throughout the European Economic Area. In accordance with article 70(1)(e) GDPR, the Board shall to this end examine on request of one of its members any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation. Article 39(6) Regulation 2018/1725 provides that, prior to its adoption, the European Data Protection Supervisor shall request the EDPB to examine - in accordance with article 70(1)(e) GDPR - the draft list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 39(4) Regulation 2018/1725. This obligation applies insofar the list refers to processing operations by a controller within the scope of article 3(8) Regulation 2018/1725 acting jointly with one or more controllers other than Union institutions and bodies. The aim of this recommendation is therefore to be coherent with the approach previously taken towards draft lists of supervisory authorities (hereinafter SAs). The Board sought to achieve consistency 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.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 39(1) Regulation 2018/1725 where processing is “likely to result in a high risk to the rights and freedoms of natural persons”. Article 39(3) Regulation 2018/1725 illustrates what is likely to result in a high risk. This is a non-exhaustive list, which corresponds with the wording of article 35(3) GDPR. 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.

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.

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 European Data Protection Supervisor supports 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 are relevant.

HAS ADOPTED THE FOLLOWING RECOMMENDATION:

1 SUMMARY OF THE FACTS

1. The European Data Protection Supervisor has submitted its draft list, in application of Article 39(4) Regulation 2018/1725, to the EDPB on 18 March 2019 and submitted a revised version on 21 June 2019.
2. The document submitted by the European Data Protection Supervisor also included a part relating to Article 39(5) of Regulation 2018/1725. The revised draft document explicitly specifies that the Article 39(5) list included in it applies only to situations in which Union institutions or bodies are joint or sole controllers. In particular, the draft Article 39(5) list covers processing operations related to Union institutions' or bodies' processing for their internal management, undertaken without the involvement of controllers other than Union institutions and bodies.
3. Thus, the EDPB notes that this second part of the document falls outside the scope of Article 39(6) Regulation 2018/1725. This provision determines that the obligation to request a recommendation of the EDPB applies only to those items that concern processing operations where a controller subject to Regulation 2018/1725 acts jointly with one or more controllers that are not Union institutions or bodies. Thus, the EDPB will not comment on this part of the draft document.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted list

4. The list submitted to the EDPB is interpreted as further specifying Art 39.1 Regulation 2018/1725, which will prevail in any case. Thus, the list should not be considered to be exhaustive.
5. The Board takes note of article 39.10 Regulation 2018/1725, which provides that no DPIA is required if the specific processing operation or set of operations in question has a legal basis in a legal act adopted on the basis of the Treaties, and where a data protection impact assessment has already been carried out as part of a general impact assessment preceding the adoption of that legal act. In this case the paragraphs 1 to 6 of article 39 shall not apply unless the legal act in question provides otherwise.
6. This recommendation does not, as a general principle, reflect upon items submitted by the European Data Protection Supervisor, which were deemed outside the scope of Article 39.6 Regulation 2018/1725. This refers to items that do not concern the processing operation where a controller acts jointly with one or more controllers that are not Union institutions or bodies. However, since the European Data Protection Supervisor has decided to adopt one list for both kinds of processing

operations, the present recommendation does de facto apply to both categories of processing activities.

7. The recommendation aims to align with the core of processing operations, which the Board requested all Supervisory Authorities to add to their list, if not already present.
8. This means that, for a limited number of types of processing operations that will be defined in a harmonised way, the Board recommends the European Data Protection Supervisor to require a DPIA to be carried out.
9. When this recommendation remains silent on DPIA list entries submitted, it means that the Board is not suggesting the European Data Protection Supervisor to take further action.
10. 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 recommends including an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines to improve transparency.

2.2 Analysis of the draft list

11. Taking into account that:
 - a. Article 39 (1) Regulation 2018/1725 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 39 (3) Regulation 2018/1725 provides a non-exhaustive list of types of processing that require a DPIA,

the Board issues the following recommendations:

SENSITIVE DATA

12. The draft list cites 'sensitive data' as a criterion as follows "Sensitive data: data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for uniquely identifying a natural person, data concerning health or sex life or sexual orientation, criminal convictions or offences and related security measures or otherwise considered sensitive."
13. Although the wording is very similar to the DPIA Guidelines of the A29WP WP248rev.01, endorsed by the EDPB, there is a significant difference. Where the draft list uses the wording "or otherwise considered sensitive", the guidelines state "data of a highly personal nature".
14. The Board notes that the GDPR does not use the term 'sensitive data' in any of the articles, though it is mentioned in 2 recitals, the term is understood to exclusively designate the categories of data listed in article 9 and 10 GDPR. In order to avoid confusion, the Board recommends the European Data Protection Supervisor to amend the wording 'or otherwise considered sensitive' and use the exact wording of the DPIA guidelines.

LARGE SCALE PROCESSING

15. The Board notes that the European Data Protection Supervisor makes reference to the internal phone directory of an EU institution as a counterexample of large scale processing. Without prejudice as to whether a DPIA is indeed required, it is not clear why a phone directory of an EU institution does not per se fall within the notion of large scale processing, especially since it can potentially include personal

data of a large number of individuals. The EDPB also reminds that the notion of large also refers to the proportion of the relevant population, as defined in Guidelines on Data Protection Officers ('DPOs'), adopted in December 2016, revised on 5 April 2017, and endorsed by the EDPB. The Board recommends the use of a different example.

DATASETS MATCHED OR COMBINED FROM DIFFERENT DATA PROCESSING OPERATIONS

16. The Board notes that the example used for processing operations that involve datasets matched or combined from different data processing operations might raise doubts regarding its lawfulness under Regulation 2018/1725, given the way it is described. Whilst the Board is not in the position and does not have the competence to assess this lawfulness, it recommends, for the sake of clarity, the use of a different example.

VULNERABLE DATA SUBJECTS

17. The Board notices that the European Data Protection Supervisor uses in his decision as a counterexample of EU institutions staff *vis-a-vis* the standard procedures laid down in the Staff Regulations. The Board recalls that employees are listed as vulnerable data subjects in the DPIA Guidelines of the A29WP WP248rev.01, endorsed by the EDPB. Though it is arguable that the power imbalance between an employer and an employee is less acute in the context of 'standard procedures' under the relevant Staff Regulations, this cannot be considered always to be the case, especially when the employees do not have significant influence on the content of said Regulations. In addition, it is not clear which procedures may be considered as non-standard, in which case a DPIA would potentially be needed, which might result in significant confusion. For these reasons, the Board recommends that the European Data Protection Supervisor replace the counterexample given with a different one.

3 CONCLUSION

18. The Board invites the European Data Protection Supervisor to make the following changes to its list:
-) Regarding sensitive data: the Board recommends the European Data Protection Supervisor to amend its list by modifying the wording “or otherwise considered sensitive” and use the exact wording of the DPIA guidelines;
 -) Regarding data processed on a large scale: the Board recommends to the European Data Protection Supervisor to amend its list by using a different counterexample ;
 -) Regarding datasets matched or combined from different data processing operations: the Board recommends to the European Data Protection Supervisor to amend its list by using a different example ;
 -) Regarding vulnerable data subjects: the Board recommends to the European Data Protection Supervisor to amend its list by using a different counterexample ;

For the European Data Protection Board

The Chair

(Andrea Jelinek)