

Opinion of the Board (Art. 64)



EDPB Plenary Meeting, 22-23 January 2019

Opinion 01/2019 on the draft list of the competent supervisory authority of the Principality of Liechtenstein regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)

Adopted on 23 January 2019

Table of 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
	BIOMETRIC DATA	6
	GENETIC DATA.....	6
	PROCESSING USING INNOVATIVE TECHNOLOGY	6
	SYSTEMATIC TRACKING	7
	COMBINING OR MATCHING PERSONAL DATA OBTAINED FROM MULTIPLE SOURCES AND FURTHER PROCESSING THEREOF.....	7
	SYSTEMATIC WORKPLACE MONITORING	7
	EXCEPTIONS TO INFORMATION TO BE PROVIDED TO THE DATA SUBJECT ACCORDING TO ARTICLE 14.5 GDPR	7
	DENIAL OF SERVICE BASED (NOT SOLELY) ON AUTOMATED DECISION-MAKING (INCLUDING PROFILING).....	8
	PROCESSING OF PERSONAL DATA IF THE DATA ARE EVALUATED, PROCESSED AND USED BY THE AUTHORITIES CONCERNED AND FORWARDED TO LAW ENFORCEMENT AUTHORITIES.....	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 (hereafter “GDPR”),

Having regard to Article 51 (1b) of Directive 2016/680 EU on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereafter “Law Enforcement Directive”).

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, 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 (hereafter GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) 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 harmonised 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 received an opinion on their draft lists from the EDPB on 5 September 2018. A further 4 SAs received an opinion on their draft lists on 7 December 2018.

(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 FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The competent supervisory authority of the Principality of Liechtenstein has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 29 October 2018.
2. The period until which the opinion has to be adopted has been extended until 5 February 2019 taking into account the complexity of the subject matter, in particular the need to factor in the outcome of the review of the twenty-six draft lists previously submitted by competent supervisory authorities and the need for a global assessment of all of them.

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

3. 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.
4. 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.
5. Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Data Protection Office of the Principality of Liechtenstein (hereafter Liechtenstein Supervisory Authority) shall add a reference to this measure.
6. This opinion does not reflect upon items submitted by the Liechtenstein Supervisory Authority, 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.
7. 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 GDPR, the Board will not comment on those local processing.
8. The Board notes that types of processing which fall within the scope of the Law Enforcement Directive are by definition not subject to article 35.6 GDPR, however the Board may issue recommendations based on article 51 (1b) of the Law Enforcement Directive.
9. The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.
10. 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.
11. When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Liechtenstein Supervisory Authority to take further action.
12. 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 Liechtenstein Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

13. The draft list submitted by the Liechtenstein Supervisory Authority 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

14. 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:

BIOMETRIC DATA

15. The list submitted by the Liechtenstein Supervisory Authority for an opinion of the Board states, that the extensive 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 is not necessarily likely to represent a high risk per se. 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. The Board is of the opinion that the wording used to describe the type of processing is not clear enough. Either the extensive nature of the processing means that the processing is made on a large scale, in which case the description should be modified to clearly make a reference to this criterion, or it just means that the criterion is systematically used, in which case another criterion should be added to ensure consistency.

GENETIC DATA

16. The list submitted by the Liechtenstein Supervisory Authority for an opinion of the Board does not currently require a DPIA to be done for the processing of genetic data. The Board is of the opinion that the processing of genetic data is not necessarily likely to represent a high risk per se. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. Therefore, the Board requests the Liechtenstein Supervisory Authority to amend its list accordingly, by adding explicitly the processing of genetic data in conjunction with at least one other criterion to its list, to be applied without prejudice to article 35(3) GDPR.

PROCESSING USING INNOVATIVE TECHNOLOGY

17. The list submitted by the Liechtenstein Supervisory Authority for an opinion of the Board envisages that the use of innovative technology, on its own, requires a DPIA. The Board is of the opinion that the use of innovative technology is not necessarily likely to represent a high risk per se. 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 Liechtenstein Supervisory Authority to amend its list accordingly, by adding that the item requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion.

SYSTEMATIC TRACKING

18. The Board recalls that systematic tracking is a factor in determining the likelihood of high risk, however does not necessarily lead to a likely high risk per se. However, where systematic tracking occurs in conjunction with at least one other criterion, a DPIA should be carried out. The list submitted by the Liechtenstein Supervisory Authority for an opinion of the Board does currently require a DPIA to be carried out when systematic tracking of data subjects occurs. The Board requests the Liechtenstein Supervisory Authority to amend its list accordingly, by requiring a DPIA to be carried out in cases of systematic tracking of data subjects only when it is done in conjunction with at least one other criterion.

COMBINING OR MATCHING PERSONAL DATA OBTAINED FROM MULTIPLE SOURCES AND FURTHER PROCESSING THEREOF

19. The Board recalls that matching or combining datasets is a factor in determining the likelihood of high risk, however in its view combining or matching of personal data obtained from multiple sources does not lead to a likely high risk per se. The Board further recalls that in its view further processing of personal data should not be a criterion leading to an obligation to do a DPIA, alone or with another criterion. The list submitted by the Liechtenstein Supervisory Authority for an opinion of the Board does currently require a DPIA to be carried out when combining or matching of personal data obtained from multiple sources and further processing thereof occurs. The Board requests the Liechtenstein Supervisory Authority to amend its list accordingly, by requiring a DPIA to be carried out in case of combining or matching of personal data obtained from multiple sources only when occurring in conjunction with at least one other criterion.

SYSTEMATIC WORKPLACE MONITORING

20. The Board takes note of the inclusion of “systematic workplace monitoring” in the Liechtenstein DPIA list. The Board recalls that in its view WP249 of the Article 29 working party remain valid when defining the concept of systematic processing of employee data.

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

21. 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 per se. 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) could require a DPIA to be carried out only in conjunction with at least one other criterion. The list submitted by the Liechtenstein Supervisory Authority 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) applies extensively. The Board is of the opinion that the wording used to describe the type of processing is not clear enough. Either the extensive nature of the processing means that the processing is made on a large scale, in which case the description should be modified to clearly make a reference to this criterion, or it just means that the criterion is systematically used, in which case another criterion should be added to ensure consistency.

DENIAL OF SERVICE BASED (NOT SOLELY) ON AUTOMATED DECISION-MAKING (INCLUDING PROFILING)

22. The list submitted by the Liechtenstein Supervisory Authority for an opinion of the Board states, that the processing activities which lead to a denial of service, when based, but not solely, on an automated decision (including profiling) fall under the obligation to perform a DPIA. The Board is of the opinion that the reference to automated decision-making does not count as a second criterion in this case, since the description states that the processing which include a human intervention are also included. This means that any processing that end up with a denial of service are subject to the obligation to do a DPIA. The Board therefore requests the Liechtenstein Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing which may lead to denial of service based (not solely) on automated decision-making (including profiling) requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion.

PROCESSING OF PERSONAL DATA IF THE DATA ARE EVALUATED, PROCESSED AND USED BY THE AUTHORITIES CONCERNED AND FORWARDED TO LAW ENFORCEMENT AUTHORITIES

23. The list submitted by the Liechtenstein Supervisory Authority for an opinion of the Board states, that the processing activities which are further transmitted to law enforcement fall under the obligation to perform a DPIA. The Board takes note that those processing operations will not always fall within the scope of the Law Enforcement Directive: whistle blowing processing for example, will fall under this criterion and will therefore require a DPIA. The Board acknowledges that the fact that data will likely be forwarded to law enforcement authorities can be a factor in determining the likelihood of high risk, however it does not necessarily lead to a likely high risk per se. The Board therefore requests the Liechtenstein Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing when data are evaluated, processed and used by the authorities concerned and forwarded to law enforcement authorities requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion.

3 CONCLUSIONS / RECOMMENDATIONS

24. The draft list of the Liechtenstein Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to be made:
- Regarding biometric data: the Board requests the Liechtenstein Supervisory Authority to amend its list by adding explicitly the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion to its list;
 - Regarding genetic data: the Board requests the Liechtenstein Supervisory Authority to amend its list by adding explicitly the processing of genetic data in conjunction with at least one other criterion to its list;
 - Regarding processing using new or innovative technology: the Board requests the Liechtenstein Supervisory Authority to amend its list 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;
 - Regarding systematic tracking: the Board requests the Liechtenstein Supervisory Authority to amend its list by adding that the item requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion;

- Regarding combining or matching of personal data obtained from multiple sources and further processing thereof: the Board requests the Liechtenstein Supervisory Authority to amend its list by firstly removing the reference to further processing and secondly by adding that the item requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion;
- Regarding exceptions to information to be provided to the data subject according to Art. 14.5 GDPR: the Board request the Liechtenstein Supervisory Authority to amend its list either by clarifying that the extensive nature of the processing means that the processing is made on a large scale or, if it just means that the criterion is systematically used, by adding that the item requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion;
- Regarding denial of service based (not solely) on automated decision making (including profiling): the Board requests the Liechtenstein Supervisory Authority to amend its list by adding that the item requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion;
- Regarding the data evaluated, processed and used by the authorities concerned and forwarded to law enforcement authorities: the Board requests the Liechtenstein Supervisory Authority to amend its list by adding that the item requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion

4 FINAL REMARKS

25. This opinion is addressed to the Data Protection Office of the Principality of Liechtenstein (Liechtenstein Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.
26. 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)