Opinion 6/2018

on the draft list of the competent supervisory authority of Estonia

regarding

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

Adopted on 25th September 2018

Contents

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 assessment[1], as endorsed by the EDPB[2], 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:

1. Summary of the Facts

The Andmekaitse Inspektsioon (hereafter Estonian Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 20th of June 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. As the list provided by Estonian Supervisory Authority does not explicitly state this, the Board requests this explanation to be added to the document containing the list.

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 Estonian Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Estonian 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.

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 Estonian Supervisory Authority 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 Estonian Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Estonian 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

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:

INDICATIVE NATURE OF THE LIST

As the list provided by Estonian Supervisory Authority does not explicitly state that its list is not exhaustive, the Board requests this explanation to be added to the document containing the list.

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 Estonian Supervisory Authority does not contain such a statement, the Board recommends the Estonian Supervisory Authority to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Estonian Supervisory Authority for an opinion of the Board does not currently require a DPIA to be done for the processing of biometric data for the purpose of uniquely identifying a natural person. As such, the Board requests the Estonian Supervisory Authority to amend its list accordingly, 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, to be applied without prejudice to article 35(3) GDPR.

GENETIC DATA

The list submitted by the Estonian 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 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 Estonian 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.

LARGE SCALE

The GDPR does not precisely define what constitutes large-scale. In the WP29 guidelines on Data Protection Officer and on DPIA, both endorsed by Board, it has recommended to take in account several specific factors when determining whether a processing is carried out on a large scale.

The Board is of the opinion that those factors are sufficient to assess whether the processing of personal data is undertaken on a large scale. Therefore the Board requests the Estonian Supervisory Authority to amend its list accordingly, by deleting the explicit figures in its list, and making reference to the previously mentioned definitions of large scale.

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 Estonian Supervisory Authority 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.

3. Conclusions / Recommendations

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

- Regarding the indicative nature of the list: the Board requests an explanation to be added to the document containing the list, stating its non-exhaustive nature.
- Regarding the reference to the guidelines: the Board requests the Estonian Supervisory Authority to amend its document accordingly.
- Regarding biometric data: the Board requests the Estonian Supervisory Authority to amend its list accordingly, 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 Estonian 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 the notion of large scale: the Board requests the Estonian Supervisory Authority to amend its list by deleting the explicit figures in its list, and making reference to the definitions of large scale mentioned in the WP29 guidelines on Data Protection Officer (WP243) and on DPIA (WP248).
- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.

4. Final Remarks

This opinion is addressed to the Andmekaitse Inspektsioon (Estonian Supervisory Authority) 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)