Opinion 13/2019 on the draft list of the competent supervisory authority of France regarding the processing operations exempt from the requirement of a data protection impact assessment (Article 35(5) GDPR)

Adopted on 10 July 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 5
2.3 Analysis of the draft list 5
Reference to the guidelines 6
Processing personal data in the context of Human Resources 6
Breathalyser tests and tachographs 6
Managing access controls and work schedules 6
Recovery of debt 6
Significance of the items on the 35(5) GDPR list 7
List items considered out of scope of article 35(6) GDPR 7
3 CONCLUSIONS / RECOMMENDATIONS 7
4 FINAL REMARKS 8

The European Data Protection Board

Having regard to Article 63, Article 64(2)and Article 35(1), (5), (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 Article 51(1)(b) 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, 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 compliance with Articles 35(6) and 64(2) GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to adopt a list of processing operations not subject to the requirement for a data protection impact assessment pursuant to Article 35(5) 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 by ensuring that the lists do not contradict the cases where the GDPR explicitly states that a type of processing should undergo a DPIA, by recommending SAs to remove some criteria which, the Board considers not correlated with the absence of likelihood of high risks for data subjects, by recommending them to limit the scope of the types of processing in order not to contradict the general rules defined in the DPIA guidelines from the Article 29 Working Party, endorsed by the EDPB, and finally by recommending them to use some criteria in a harmonized manner.

(2) With reference to Article 35(5) and (6) GDPR, the competent supervisory authorities may establish lists of the kind of processing operations which are not 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) The EDPB ensures pursuant to Article 70(1) of the GDPR the consistent application of Regulation 2016/679 throughout the European Economic Area. Under Article 64(2), the consistency mechanism may be triggered by a supervisory authority, the EDPB Chair or the Commission for any matter of general application or producing effects in more than one Member State. The EDPB shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter.

(4) 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 across the EEA.

(5) 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". The national SAs can issue lists concerning certain processing activities which always require a DPIA (blacklists) per Article 35(4) as well as lists where no DPIA is necessary per Article 35(5) (whitelists). When a processing does not fall within either of these two lists and is not mentioned Article 35(3) GDPR, an ad hoc decision will have to be made by the data controller based on whether the "likely to result in a high risk to the rights and freedoms of natural persons" criterion is met. According to Recital 91 of the GDPR a DPIA will not be mandatory when the processing is carried out by an individual physician, other health care professional or a lawyer, as it is not of a sufficient large scale. This exception covers only partially the cases when a DPIA will not be necessary, i.e. when there is no high risk to the rights and freedoms of natural persons.

(6) The lists produced by the competent supervisory authorities support a common objective, namely to identify the kind of processing operations for which the national SAs are certain that, under no circumstances, they will result in a high risk, and processing operations the national SAs deem unlikely to result in a high risk, and therefore do not require a DPIA. The Board refers to the Working Party 29 Guidelines on DPIA (WP248 rev.01)[1], which sets out criteria to consider in determining processing operations "*likely to result in a high risk*".[2] As set out in these guidelines, 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.

(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 France has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 20 May 2019.

2. The period until which the opinion has to be adopted has been extended until 26 August 2019.

[1] 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, adopted on 4 April 2017 and revised on 4 October 2017

[2] Recitals 75, 76, 92, 116 GDPR.

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 on the one hand Article 35 GDPR, which will prevail in any case, and on the other hand recital 91. Thus, no list can be exhaustive.

4. This opinion does not reflect upon items submitted by the French 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". However, for the sake of clarity, the Board will enumerate the items of the list, which were deemed outside the scope of Article 35(6) GDPR. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

5. This opinion will not comment on any items on the list, which fall within the scope of recital 91.

6. The opinions on the Article 35(4) GDPR lists also aimed at defining a consistent core of processing operations, which the Board requested all Supervisory Authorities to add to their list if not already present in order to ensure consistency. The article 35(5) GDPR lists may not exempt these general processing operations as a rule.

7. The lists established by SAs pursuant to Article 35(5) GDPR are inherently non-exhaustive. These lists contain types of processing regarding which national SAs are certain that, under no circumstances, they will result in a high risk to the rights and freedom of natural persons, and processing operations the national SAs deem unlikely to result in a high risk. Such lists cannot enumerate all cases in which a DPIA will not be necessary. In any event, the obligation of the controller or processor to assess the risk of the processing and to comply with the other obligations imposed by the GDPR remain applicable.

8. When this opinion remains silent on an item from the list, it means that the Board is not asking the French Supervisory Authority to take further action.

9. 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 to the criteria set out in the guidelines could improve this transparency.

2.2 Application of the consistency mechanism to the draft list

10. The draft list submitted by the French 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

11. 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

12. The Board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 is a core element for ensuring consistency across the Union. Thus, it recommends the different Supervisory 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.

PROCESSING PERSONAL DATA IN THE CONTEXT OF HUMAN RESOURCES

13. The French list includes the *"Processing operations, implemented under the conditions laid down by the applicable texts, solely for human resources purposes by employers with fewer than 250 people, except when profiling is used".* The Board notes that the processing of personal data in the context of human resources (HR data) is a broad item that might involve categories of personal data, the processing of which is likely to pose a high risk to the rights and freedoms of natural persons. However, the processing activities envisaged by the French Supervisory Authority's list are restricted to processing that are not conducted on a large scale and are mandatory by law. The Board therefore deems this list item in accordance with Article 35(5) GDPR.

BREATHALYSER TESTS AND TACHOGRAPHS

14. The French list includes *"Processing relating to breathalyser tests and tachographs implemented in the framework of transport activities".* The Board notes that the item concerning processing relating to breathalyzer tests and tachographs is broad and may involve processing which is likely to pose a high risk to the rights and freedoms of natural persons. For this reason, the Board recommends that this item be further restricted to cases where processing of such data is mandatory by law, that the purposes of the use of breathalyzer test data is restricted to the sole purpose of preventing drivers from operating vehicles while under the influence of alcohol or narcotics, and that the use of tachographs, is removed from the list.

MANAGING ACCESS CONTROLS AND WORK SCHEDULES

15. The French list includes the *"Processing carried out solely for the purpose of managing access controls and schedules, excluding any biometric device".* The Board is of the opinion that the processing activities carried out in the context of managing access controls and work schedules is a broad item that might include processing, which are likely to pose a high risk to the rights and freedoms of natural persons. Hence, the Board recommends this item be further restricted to cover only processing of data that does not reveal sensitive data or data of a highly personal nature. With respect to access control, the Board recommends restricting the scope of the item to processing activities solely in the context of standard and non-biometric mechanisms aimed at controlling physical access. Further, the Board recommends clarifying in the item that, with respect to work schedules, only processing activities with the sole purpose of calculating working times are covered.

RECOVERY OF DEBT

16. The French list includes the *"Processing operations carried out by the data controller for the recovery of its outstanding debts, and for its own account".* The Board is of the opinion that the processing activities carried out in the context of recovery of debt is a broad item that may cover processing which is likely to pose a high risk to the rights and freedoms of natural persons. The Board recommends that the French Supervisory Authority further restrict the scope of this item by stating that it does not apply to the processing activities concerning debts which have been acquired from a third party, and that it only applies to debts owed in the context of a business to consumer relationship. Furthermore, the Board recommends that evaluation and scoring be explicitly excluded from scope of this item.

SIGNIFICANCE OF THE ITEMS ON THE 35(5) GDPR LIST

17. The Board notes that the mere fact that processing activity falls within the scope of a 35(5) GDPR list does not mean that a controller is exempt from the obligations set out in Article 32 GDPR. Hence, an assessment of the risks for the rights and freedoms of natural persons, their likelihood and severity, needs to be undertaken by the controller and processor in order to ensure a level of security appropriate to the risk in compliance with Article 32 GDPR. The Board encourages the French Supervisory Authority to include in its list a paragraph making this distinction between Articles 32 and 35 of the GDPR for the sake of clarity.

LIST ITEMS CONSIDERED OUT OF SCOPE OF ARTICLE 35(6) GDPR

18. The Board is of the view that the following items on the list fall outside the scope of Article 35(6) GDPR[1] and consequently does not issue recommendations on these items.

- Processing implemented under the conditions provided by the law relating to the management of the electoral register of municipalities;
- Processing carried out by the clerks of commercial courts for the purpose of carrying out their activity;
- Processing carried out by notaries for the purpose of carrying out their notarial activity and the drafting of notarial office documents;
- Processing carried out by local authorities, as well as legal persons covered by public and private law, for the management of schools, as well as extracurricular and early childhood services.

19. Therefore, the Board does not have any comments on these items.

3 CONCLUSIONS / RECOMMENDATIONS

20. The draft list of the French Supervisory Authority may lead to an inconsistent application of Article 35 GDPR and recommends that the following changes be made:

- Regarding the reference to the guidelines: the Board recommends the Supervisory Authority of France to amend its document accordingly.
- Regarding breathalyser tests and tachographs: the Board recommends that this item be restricted to processing mandated by law, that it be restricted to the sole purpose of preventing drivers from operating vehicles while under the influence of alcohol or narcotics and that the processing involving the use of a tachograph be removed from the list.
- Regarding managing access controls: the Board recommends this item be restricted to cover only processing of data that does not reveal sensitive data or data of a highly personal nature. With respect to access control, the Board recommends restricting the scope of the item to processing activities solely in the context of standard and non-biometric mechanisms aimed at controlling physical access. Further, the Board recommends clarifying in the item that, with respect to work schedules, only processing activities with the sole purpose of calculating working times are covered.
- Regarding recovery of debt: the Board recommends the exclusion from this item of evaluation and scoring as well as exclusion of debts acquired from a third party , and further to restrict the item to debts owed in the context of a business to consumer relationship.

[1] This view is strictly tied to the present list and does not apply necessarily to similar items in the lists submitted by other Supervisory Authorities.

- Regarding the significance of items listed: the Board encourages the French Supervisory Authority to clarify that its list is without prejudice to any other obligation stipulated by the GDPR.

4 FINAL REMARKS

21. This opinion is addressed to the Commission Nationale de l'Informatique et des Libertés (French Supervisory Authority) and will be made public pursuant to Article 64(5)(b) GDPR.

22. The French Supervisory Authority shall communicate the final decision to the Board for inclusion in the register of decisions which have been subject to the consistency mechanism, in accordance with Article 70(1)(y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)