EVALUATION OF THE GDPR UNDER ARTICLE 97 – QUESTIONS TO DATA PROTECTION AUTHORITIES / EUROPEAN DATA PROTECTION BOARD

ANSWERS FROM THE NORWEGIAN SUPERVISORY AUTHORITY

The General Data Protection Regulation ('GDPR') entered into application on 25 May 2018, repealing and replacing Directive 95/46/EC. The GDPR aims to create a strong and more coherent data protection framework in the EU, backed by strong enforcement. The GDPR has a two-fold objective. The first one is to protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. The second one is to allow the free flow of personal data and the development of the digital economy across the internal market.

According to Article 97 of the GDPR, the Commission shall submit a first report on the evaluation and review of the Regulation to the European Parliament and the Council. That report is due by 25 May 2020, followed by reports every four years thereafter.

In this context, the Commission shall examine, in particular, the application and functioning of:

- Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC; and
- Chapter VII on cooperation and consistency.

The GDPR requires that Commission takes into account the positions and findings of the European Parliament and the Council, and of other relevant bodies and sources. The Commission may also request information from Member States and supervisory authorities. As questions related to Chapter VII concern more directly the activities of the DPAs, the present document focuses primarily on that aspect of the evaluation, while also seeking their feedback on Chapter V related issues.

We would be grateful to get the replies to the questions (in English) by 15 January 2019, at the following e-mail address: JUST-EDPB@ec.europa.eu.

Please note that your replies might be made public.

When there are several DPAs in a given Member State, please provide a consolidated reply at national level. In the context of the preparation of the evaluation report, and following the input from other stakeholders, it is not excluded that we might have additional questions at a later stage.

I. CHAPTER V

The GDPR provides that the adequacy decisions adopted by the Commission under Directive 95/46 remain in force under the GDPR until amended, replaced or repealed. In that context, the Commission is tasked to continuously monitor and regularly evaluate the level of protection guaranteed by such decisions. The 2020 evaluation provides a first opportunity to evaluate the 11 adequacy decisions adopted under the 1995

Directive. This does not include the decision on the Privacy Shield that is subject to an ad hoc annual review process and the Japanese adequacy decision that was adopted last year under the GDPR and is also subject to a specific evaluation exercise (the first one will be in 2021).

1. Has any stakeholder raised with your authority any particular question or concern regarding any of the adequacy decisions adopted under the 1995 Directive (with the exception of the EU-US adequacy decision which is not covered by this evaluation process)?

No.

2. Does your authority have any information on the developments of the data protection system of any of the countries/territories subject to a Commission adequacy decision under the 1995 Directive that you would consider relevant for the Commission's evaluation?

No.

3. In your view, should any third country or international organisation be considered by the Commission in view of a possible adequacy decision?

International Organization for Migration (IOM)

II. CHAPTER VII

The GDPR provided for one single set of data protection rules for the EU (by a Regulation) and one interlocutor for businesses and one interpretation of those rules. This "one law one interpretation" approach is embodied in the new cooperation mechanism and consistency mechanisms. In order to cooperate effectively and efficiently the GDPR equips the Data Protection Authorities (thereafter the DPA/DPAs) with certain powers and tools (like mutual assistance, join operations). Where a DPA intends to adopt a measure producing effects in more than Member State, the GDPR provides for consistency mechanism with the power to ask for opinions of the European Data Protection Board (EDPB) on the basis of Article 64(1) and (2) GDPR. In addition, in situations where the endeavour to reach consensus in the cases of one-stop shop (OSS) does not work (i.e. there is a dispute between the DPAs in specific cases), the EDPB is empowered to solve the dispute through the adoption of binding decisions.

In this context, the Commission finds it appropriate to request the views of the DPAs / EDPB on their first experiences on the application of the cooperation and consistency mechanisms. To this aim, the Commission established the list of questions below, in order to help the DPAs framing their input. It is understood, that the Commission is also interested in any comments the DPAs may have which goes beyond the answer to the questions and which concerns the application of the two above-mentioned mechanisms.

1. Cooperation Mechanism

1.1. OSS – Article 60

a. Has your DPA been involved in any OSS cases? If so, in how many cases since May 2018?

The NO SA has been identified as CSA in 734 OSS cases (a large number of those cases are not in the case register). This number has been calculated on the basis of Article 56 Identification processes in IMI.

The NO SA has been identified as LSA in 8 OSS cases.

b. Did you encounter any problems/obstacles in your cooperation with the lead/concerned DPA? If yes, please describe them

No.

c. How would you remedy these problems?

N/A

d. Is your national administrative procedure compatible with the OSS? (e.g. do you identify a clear step which can be referred to as a "draft decision"? Are the parties heard before you produce such draft decision?)

Pursuant to Norwegian administrative law, we have to notify any decision before adopting it, which in essence means that we need to provide a draft decision to the controller. Under the GDPR, we are required to prepare a draft decision for CSAs as well. Therefore, we may end up creating two draft decisions. If feedback on one of the draft decisions lead to substantial changes in our conclusions, we may need to resubmit a draft decision to either the controller or the CSAs, which again may invite new feedback. We would consider the national procedure to be compatible with the OSS.

e. Were you in the situation of the application of the derogation provided for in Article 56(2) GDPR (so-called "local cases", i.e. infringements or complaints relating only to an establishment in your Member State or substantially affecting data subjects only in your Member State)?

Yes. This applied in a delisting (right to be forgotten) case in the Yahoo search engine, for which IE SA is LSA.

f. Is the OSS living up to its expectations? If not, what would you identify as its shortcomings? How can they be remedied?

It lives up to its expectation, but it requires more resources and takes more time than originally anticipated.

1.2. Mutual assistance – Article 61

a. Did you ever use this tool in the case of carrying out an investigation?

We have not used it ourselves, but we have received requests from other SAs in the context of their investigations.

b. Did you ever use this tool in the case of monitoring the implementation of a measure imposed in another Member State?

No.

c. Is this tool effectively facilitating your work? If yes, how? If not, why?

Yes. It provides a secure and efficient way (with deadlines) to communicate in the context of a particular case.

d. Do you encounter any other problems preventing you from using this tool effectively? How could they be remedied?

No.

1.3. Joint operations – Article 62

a. Did you ever use this tool (both receiving staff from another DPA or sending staff to another DPA) in the case of carrying out and investigation?

No.

b. Did you ever use this tool in the case of monitoring the implementation/enforcement of a measure imposed in another Member State?
No.

c. Is it effectively facilitating your work? If yes, how? If not, why?
N/A

d. Did you encounter any problems (e.g. of administrative nature) in the use of this tool? How could they be remedied?
N/A

2. Consistency mechanism

a. Opinion - Article 64 GDPR

a. Did you ever submit any draft decision to the Board under Art 64(1)?
Yes (list of processing operations subject to the requirement for a data protection impact assessment)

b. Did you ever submit any draft decision to the Board under Art 64(2)?
No.

c. Did you have any problems by complying with the obligations under Article 64(7) GDPR, i.e. taking outmost account of opinion of the EDPB? If so please describe them.
No.

d. Was the "communication of the draft decision" complete? Which documents were submitted as "additional information"?
It was complete. N/A

e. Were there any issues concerning the translations and/or any other relevant information?
Not in this case, since the list was written in English. Translation issues may arise in other cases.

f. Does that tool fulfil its function, namely to ensure a consistent interpretation of the GDPR?
Yes.

b. Dispute resolution - Article 65 GDPR

a. Was this procedure used? If yes, what was your experience during the process?
No. N/A

b. Which documents were submitted to the EDPB?
N/A

c. Who prepared the translation, if any, of that documents and how much time did it take to prepare it? Were all the documents submitted to the EDPB translated or only some of them?
N/A

c. Urgency Procedure – Article 66

a. Did you ever adopt any measure under urgency procedure?
No.

3. Exchange of information: Standardised communication

a. What is your experience with the standardised communication through the IMI system?
This is a useful tool. However, there are significant variations as to how much and detailed information the different SAs provide.

4. **European Data Protection Board**
   a. Can you provide an indicative breakdown of the EDPB work according to the tasks listed in Article 70?
   b. *For the EDPB Secretariat*: Can you provide an indicative breakdown of the EDPB Secretariat work and allocation of resources (full-time equivalent) according to the tasks listed in Article 75?

5. **Human, technical and financial resources for effective cooperation and participation to the consistency mechanism**
   a. How many staff (full-time equivalent) has your DPA? Please provide the figures at least for 2016, 2017, 2018, 2019 and the forecast for 2020.
      2016: 48
      2017: 48
      2018: 43
      2019: 49
      2020: ≈ 57,5
   b. What is the budget of your DPA? Please provide the figures (in euro) at least for 2016, 2017, 2018, 2019 and the forecast for 2020.
      2016: € 4 512 660
      2017: € 5 012 750
      2018: € 5 386 140
      2019: € 5 708 950
      2020: € 6 580 660
   c. Is your DPA dealing with tasks beyond those entrusted by the GDPR? If yes, please provide an indicative breakdown between those tasks and those entrusted by the GDPR.
      The NO SA deals with national data protection legislation where such legislation is permitted by the GDPR, mainly in relation to processing of personal data in the employment context. We are also responsible for enforcing the national implementation of the LED (secret services excluded) plus participating in coordinated supervision with SIS II, VIS and EURODAC. Finally, we have enforcement powers pursuant to the Norwegian Credit Data Act.
   d. How would you assess the resources from your DPA from a human, financial and technical point of view?
      We have experienced an increase in resources to meet the new workload.
   e. More specifically, is your DPA properly equipped to contribute to the cooperation and consistency mechanism? How many persons work on the issues devoted to the cooperation and consistency mechanism?
      Currently: 5. As of February 2020: 7. These personnel are also responsible for participation in the EDPB and international transfers.

6. **Enforcement**
   a. How many complaints (excluding request for information) did you receive since May 2018? What kind of communication with you/request do you qualify as a complaint?
      729.
      We consider as complaints enquiries by natural persons regarding processing of their personal data in violation of the GDPR.
   b. Which corrective powers did you use since May 2018?
      Article 58(2) (b), (c), (d), (g), (i).

c. Are you resolving any possible infringements of the Regulation with the help of so-called "amicable settlements"?
   No.

d. How many fines did you impose since May 2018? Please provide examples.
   3.
   Example: A case related to computer files with usernames and passwords to user accounts in Bergen municipality's primary schools. Due to insufficient security measures, these files had been unprotected and openly accessible. The lack of security measures in the system made it possible for anyone to log in to the school's various information systems, and thereby to access various categories of personal data relating to the pupils and employees of the schools. € 170 000.

e. Which attenuating and or aggravating circumstances did you take into account?
   In the example above, an aggravating circumstance was that the municipality was previously made aware that its security of processing was flawed and that two-factor authentication would be necessary.

Data breach statistics under the GDPR:
(please note that the GDPR became applicable in Norway on 20 July 2018, not 25 May)

2018	July	38
	August	133
	September	171
	October	213
	November	130
	December	136
2019	January	144
	February	177
	March	167
	April	108
	May	146
	June	237
	July	121
	August	124
	September	176
	October	198
	November	168

Total DBN since 20 July 2018: 821 (2018) + 1766 (2019) = 2587

Update: No. of DBN December 2019: 127. Total since 20 July 2018: 2714