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

ANSWERS FROM THE FINNISH 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?

    - No.

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?

    - Yes, we have. The Finnish DPA is considered as CSA in **270** OSS cases and as LSA in **8** OSS cases submitted into IMI.

b. Did you encounter any problems/obstacles in your cooperation with the lead/concerned DPA? If yes, please describe them
    - One of the main challenges seems to relate to national interpretations of essential definitions of the OSS mechanism and related case handling, for instance, “complaint”, “draft decision” and “amicable settlement”. For example, the different interpretation of the obligation to handle complaints lodged by data subjects in accordance with Art 77 GDPR has led to a situation where the LSA would simply refuse to handle complaints submitted to it in accordance with the Art 56.
    - Also, the national administrative procedural laws seem to affect the effective functioning of the OSS mechanism. For instance, we have encountered situations where the LSA would just stop the proceeding without submitting draft decision of the OSS case to the CSAs. For that reason, the CSA are prevented to give their view (in form of relevant and reasoned objection) whether the GDPR was infringed or not etc.

c. How would you remedy these problems?
    - Ensure common interpretation of the GDPR and making sure there is no national legislation preventing the effective implementation of the Regulation. Also ensuring the DPAs have sufficient recourses to contribute to the cross-border work.

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?)
    - In our opinion, our administrative rules are compatible with the OSS i.e. there are no applicable rules possibly hampering the effective implementation of the OSS mechanism.

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)?
    - No, we haven’t yet made use of that derogation.

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

- Generally, the OSS is functioning as expected (quite well). As described in the para b, we see that one of the main challenges of the OSS is that even though it provides legal framework for administrative cooperation, the administrative procedural rules differ, even substantially, between Member States. We understand that the harmonisation of the administrative procedural rules doesn’t fall under the competence of the EU, so the question is not easily tackled in the EU-level.
- We feel that the mechanism is still new and needs a bit more time to be fully implemented.
- In our experience the companies have some challenges in defining the controller in situations where the company is established in more than one Member State i.e. the processing would be considered as cross-border on the bases that the controller is established on more than one Members State.

1.2. Mutual assistance – Article 61

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

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?
   - In our opinion, yes. The tool provides a clear formal procedure to submit inquires to other SAs and cooperate with them. We find it effective also in a sense that in case the other SA wouldn't response or act upon the request there is clear legal grounds move forward (Art 64).

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

2. Consistency mechanism

2.1 Opinion - Article 64 GDPR

a. Did you ever submit any draft decision to the Board under Art 64(1)?
   - Yes, before adopting the list of processing operation 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”?
    - Yes.

e. Were there any issues concerning the translations and/or any other relevant information?
    - No

f. Does that tool fulfil its function, namely to ensure a consistent interpretation of the GDPR?
    - Yes, in our opinion the Art 64 procedure has fulfilled its function.

2.2 Dispute resolution - Article 65 GDPR

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

b. Which documents were submitted to the EDPB?

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?

2.3 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?
    - We think the IMI system works quite well and we welcome the improvements made since it was introduced for the first time. We think that important factor of successful use of the system is IMI Helpdesk, which provides timely assistance in case of any issues using the system.

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.

   The number also includes administrative personnel
   2016: 21
   2017: 23
   2018: 27
   2019: 45
   Forecast for 2020: 55

   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: 1,8 million
   2017: 1,9 million
   2018: 2,4 million
   2019: 3,5 million
   Forecast for 2020: 4,5 million

   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 Finnish DPA has general competence in supervising and enforcing the matters relating to processing of personal data, including the processing that doesn't fall into the competence of the EU. More precisely:
  - Law enforcement Directive implementation law,
  - e-Privacy directive implementation law (corporate or association subscribers' processing of traffic fata, location data, directory inquiry services, spam (also legal personalities), processing of personal data relating to traffic management data and cookie consent),
  - PNR Directive implementing law
  - Processing of personal data out of EU competence
  - Coordinated supervision of EU agencies and large scale systems
  - Government registers (processing of personal data)
  - In accordance with the national credit institution legislation, the Finnish DPA also has a duty to supervise the processing of credit data of legal personalities.

- FI (supervising the processing of personal data that occurs in accordance with research specific laws)
- Supervision of data protection on labour life
- Supervision of identification services

d. How would you assess the resources from your DPA from a human, financial and technical point of view?

We are is still lacking sufficient human resources. However, we foresee recruiting new personnel in 2020.

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?

- We don't have case handlers working only on the OSS cases. The case handlers are dealing with both national and cross-border cases, DBN, inspections, prior consultations and so on. We have specific internal group established for implementing the EDPB guidance on the cooperation and consistency mechanism in our DPA level and for helping all the case handlers in possible questions relating the cooperation and consistency mechanism. We have also appointed persons responsible for each EDPB expert subgroup.
- We have one expert allocating significant time on IMI related matters (assessing our role in accordance with Art 56 and checking the IMI system, helping the case handlers to upload documents and start proceedings etc). Also, we have one senior expert coordinating the international matters, including the cooperation and consistency matters.
- For these reasons it is hard to give any specific number, but there is approx. 20 people involved in these issues.

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?

- 1308 complaints since May 2018.
- We define a complaint as an action filed by data subject on alleged infringement of data protection rules that concerns processing of his/her personal data. We believe that our definition is in line with the EDPB Guidelines on local cases and - when applicable - the Art 77 GDPR**.**

b. Which corrective powers did you use since May 2018?

- We have ordered the controller to communicate a data breach to data subject
- We have issued reprimands
- We have ordered the controller to bring processing operations into compliance with GDPR
- We have ordered the controller to comply with the data subject's request to exercise his or her rights pursuant to GDPR
- We have ordered the rectification or erasure of personal data or restriction of processing pursuant to Art 16, 17
- We have also power to issue conditional fines

c. Are you resolving any possible infringements of the Regulation with the help of so-called "amicable settlements"?

- In principle, amicable settlement is not expressly defined in legislation concerning administrative proceedings. We have interpreted applicable administrative rules and principles in a way that the complainant has always the right to withdraw his/her complaint. For example, if the controller complies with the data subjects request, after we have contacted the controller, and the data subject has no more nor other claims against the controller, and also taking into account that there is no need for special legal protection, the complaint would be deemed to be settled. It should be noted that the amicable settlement happens between the parties in these cases.
- We wouldn't continue proceedings except if there is a relevant reason to do so, for example we have received other similar complaints, the complaint reveals also other infringements that would possible have wider consequences or impacts to the rights and freedoms of other data subjects as well. In those cases, we would, in principle, start the investigation from our own initiative.

d. How many fines did you impose since May 2018? Please provide examples.

- None

e. Which attenuating and or aggravating circumstances did you take into account?

N/A

Additional questions

- **National statistics on data breaches**

The Finnish SA has received 5762 data breach notifications between 25 May 2018 and 30 November 2019

- **National initiatives to give guidance to SMEs or any other specific support to the SMEs**

Re the national initiatives to give guidance to SMEs or any other specific support for the SMEs, we have cooperated various ways with stakeholders from public and private sector. For instance, we have provided our comments on sector-specific guidance and we have organized seminars for the stakeholders. We have

also participated number of seminars as speakers. We have paid a specific attention to build our website in a manner which would best serve the needs of SMEs (also of course the data subjects) and we update the website/guidance based on the feedback given by the users. At the moment, we are also finalizing our DPIA-tool directed specifically to needs of SMEs. We have also launched monthly newsletter and established a phone service to provide general guidance and advice for the data subjects and different stakeholders. We have just recently introduced separate phonelines for controllers and processors.