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

ANSWERS FROM THE ESTONIAN 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
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?

-

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?)
   Yes, generally it is (the Administrative Procedure Act refers to draft decision and hearing the party)
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
f. Is the OSS living up to its expectations? If not, what would you identify as its shortcomings? How can they be remedied?
   Too early to evaluate, we have had only a few cases, where we have been as CSA or LSA.

1.2. Mutual assistance – Article 61

a. Did you ever use this tool in the case of carrying out an investigation?
   No (not before December 2019)
b. Did you ever use this tool in the case of monitoring the implementation of a measure imposed in another Member State?
   Yes
c. Is this tool effectively facilitating your work? If yes, how? If not, why?
   We don't have enough practice to give any assessments
d. Do you encounter any other problems preventing you from using this tool effectively? How could they be remedied?
   -

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?
   We don't have enough practice to give any assessments
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

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.
We were the very first ones to submit the DPIA list, thus there were some unclear requirements and misunderstandings that were solved later (e.g. a numerical proportion of the obligation included in the original Estonian DPIA list)

d. Was the "communication of the draft decision" complete? Which documents were submitted as "additional information"?
Yes, we submitted some additional documents (e.g. chapter from our guidance)

e. Were there any issues concerning the translations and/or any other relevant information?
We had to translate the DPIA list and additional documents by ourselves, the decision was translated by the EDPB

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

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?
There is a huge amount of incoming messages, most of which we have no commitment.

4. **European Data Protection Board**
   a. Can you provide an indicative breakdown of the EDPB work according to the tasks listed in Article 70?
   This question need clarification. If you mean how many staff are dealing with EDPB and its' subgroups, then the numbers are following: 7 officials are occupied with plenary and subgroups, but none of them are full-time occupied with the EDPB issues.
   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.
   Full-time officials:
   2016 – 18
   2017 – 18
   2018 – 16
   2019 – 16
   2020 – 18

   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 – 699 821 EUR
   2017 – 699 821 EUR
   2018 – 699 482 EUR
   2019 – 750 331 EUR
   2020 – 750 331 EUR

   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.
   Yes, we are also dealing with:
   1) Freedom of Information (FOI) matters and re-use of public sector information;
   2) Law Enforcement Directive and its' implementing act;
   3) e-Privacy Directive implementation law;
   4) Coordinated supervision of EU agencies and large scale systems together with the EDPS (ie. Europol, SIS II, VIS, Eurodac, CIS, etc.) ;
   5) coordinating state and local government databases/registers;
   6) Scientific research specific laws (being member of Estonian Committee on Bioethics and Human Research, member of Statistical Council);
   7) Accessibility of the websites and mobile applications of public sector bodies (Directive 2016/2012).

   For example in 2018 we received 2384 information requests – 2161 about the data protection and spams, and 223 about the FOI matters. As for the staff, we don't have a very clear distinction between these tasks.

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

As you can see from the previous answer there has not been increase in the number of staff and financial resources. This is definitely a challenge to cover all the procedures coming from GDPR.

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?
As for November 30, 2019 we had 9 (head, senior and leading) inspectors, each with their own area of supervision. This means that each of them is also devoted to the cross-border cases accordingly to their supervision area.

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?
Number of complaints 25 May 2018 – 30 Nov 2019: 551
Complaint is a communication where a person calls for the protection his/hers rights. The complaint has to be signed and meet certain requirements.

b. Which corrective powers did you use since May 2018?
Precepts (with penalty payments), orders to comply with data subject's requests to exercise individual rights, orders to bring processing operations into compliance, orders of rectification or erasure or restriction of processing, and notification to recipients, warnings and reprimands.

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.
No fines imposed

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

-

***DATA BREACH NOTIFICATIONS** from 25 May 2018 to 30 Nov 2019: 171*

*As for the **support for SMEs**, Estonian SA has:*

- *issued guidance materials, incl. GDPR DPIA art 35.5 list;*
- *conducted consultations;*
- *conducted joint-trainings with different professional associations;*
- *hot-line for data subjects and data controllers/processors;*
- *being an initiative partner to develop further trainings for DPOs (by the major universities in Estonia).*