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

ANSWERS FROM THE AUSTRIAN 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?

   South Korea, Mexico

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. Since 25 May 2018 to 30 November 2019, the AT SA has been CSA in 709 cases and LSA in 15 cases. The number of the CSA cases results from the number of the cases uploaded on IMI in the Art. 56 GDPR procedure (Art. 4.22 lit. c GDPR) and those Art. 56 GDPR procedures, in which the AT SA

declared itself as CSA (Art. 4.22 lit. a and b GDPR). The number of LSA cases results from the number of cases on IMI, in which the AT SA declared itself as LSA (Art. 56.1 GDPR).

b. Did you encounter any problems/obstacles in your cooperation with the lead/concerned DPA? If yes, please describe them
Yes, regarding:
- the duration of the proceedings;
- missing information/documents provided by SAs as there is no unified approach;
- difficulties in the conduct of proceedings as there are questions about the application and design of the different national administrative procedural laws.

c. How would you remedy these problems?
- **Regarding the duration of proceedings and missing information:** We try to get in contact with our counterparts, first in informal ways (Email, telephone call) and then via IMI (Voluntary Mutual Assistance requests).
- **Regarding questions about the application and design of the national administrative procedural law:** We try to get in in contact with our counterparts first in informal ways (Email, telephone call) and then via IMI (Voluntary Mutual Assistance requests). Furthermore, the SAs are trying to resolve these matters on EDPB level, especially in expert subgroups (Cooperation, Enforcement or IT Users).
Nevertheless, it must be stressed that these efforts cannot substitute the fact that the GDPR itself does not contain any collision norms.

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?)
The AT SA is bound by strict procedural laws regarding the right to be heard. Thus, as a rule, every party is heard (to the facts, not the law) before a decision is drafted by the AT SA, although this draft decision is subsequently not sent to the parties prior to the issuing, just to the CSAs.

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, various times.

f. Is the OSS living up to its expectations? If not, what would you identify as its shortcomings? How can they be remedied?
Yes, but:
- There are no clear provisions regarding the communication and exchange of information among all CSA prior to a draft decision, respectively they are interpreted differently by the SAs.
- Furthermore, the OSS mechanism does not provide for clear guidance on the applicable national procedural laws. Therefore, different or even contradicting procedural laws can lead to contradicting approaches resolving a specific case, e.g. when the lodging CSA has to issue the final decision (dismissal and rejection of the complaint) that can be appealed before the national authorities.

1.2. Mutual assistance – Article 61

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

b. Did you ever use this tool in the case of monitoring the implementation of a measure imposed in another Member State?
Yes, e.g. to ask the initiating CSA to send a document to the complainant and ask for his/her statement (right to be heard) as well as for the exchange of further information.

c. Is this tool effectively facilitating your work? If yes, how? If not, why?
Yes, see question above. The AT SA used it get in contact with other SAs in an informal and formal way. The informal one was through email or a telephone call, the formal one through the IMI system. The IMI system was used to e.g. gather information or to assign a case to another SA.

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 an investigation?
No, as there are no provision in Austrian national law implementing Art. 62 GDPR.

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

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?
No, see answer to question above.

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.
No.

d. Was the "communication of the draft decision" complete? Which documents were submitted as "additional information"?

No, it was not immediately considered as complete. In these cases an English translation of the provisions of the AT national law that the draft decision referred to were submitted as additional information.

e. Were there any issues concerning the translations and/or any other relevant information?
Please see the answer above.

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

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?
See answer to question above.

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?
See answer to question above.

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?
Good, but constant improvements as well as the observation of new proceedings are necessary. The IT User Expert subgroup is working on these issues together with DG GROW.

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: 23.3
2017: 25.4
2018: 31.8
2019: 33.9
forecast 2020: 33.9

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: € 1,403,000 (€ 1,360,000 personnel expenses, € 43,000 operating expenses)
2017: € 1,765,000 (€ 1,722,000 personnel expenses, € 43,000 operating expenses)
2018: € 1,939,000 (€ 1,695,000 personnel expenses, € 244,000 operating expenses)
2019: € 2,282,000 (€ 2,039,000 personnel expenses, € 243,000 operating expenses)
forecast 2020: € 2,282,000 (€ 2,039,000 personnel expenses, € 243,000 operating expenses)

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, the AT SA is also dealing with tasks entrusted to it by the law enforcement directive implementation law.

d. How would you assess the resources from your DPA from a human, financial and technical point of view?
By far not enough.

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?
No. In total 11 lawyers and 2 administrative employees work on issues devoted to cooperation and consistency. A lawyer of the AT SA is dealing with more than 100 cases (national and cross-border) simultaneously at an average.

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?

Time frame: 25 May 2018 – 30 November 2019

Complaints lodged with the AT SA: 2807 (2484 complaints regarding only a national processing, 323 with a potential cross-border processing). Additionally the AT SA received 1142 notifications of complaints via IMI (including 15 cases to be handled as LSA).

The Austrian data protection law has very concrete provisions on submissions to be qualified as complaints. A mere request, for example as to how AT SA would qualify a case or how the legal situation looks like, is not counted as a complaint and is therefore not included in the above mentioned figures. All 2807 complaints received were followed by a substantive examination and finally an official decision.

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

Art. 58.2 lit. a, b, c, d, e, f, g and i GDPR.

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

Yes, possible infringements regarding data subject rights can be resolved, in accordance with § 24.6 of the Austrian data protection law.

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

38 fines were issued. The lowest fine imposed was € 200,-- (missing marking of a video surveillance by a natural person). The highest fine amounted to € 18,000,000,-- (unlawful processing of special categories of personal data by the Austrian Post). Most of the fines were imposed for unlawful video surveillance (violations of Art. 5.1 lit. a and Art. 5.1 lit. c in conjunction with Article 6.1 of the GDPR).

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

- **Attenuating circumstances:** integrity, a one-time misconduct, subsequent elimination or restoration of the lawful conditions, measures taken to avoid an infringement in the future, collaboration in the proceedings, confession

- **Aggravating circumstances:** highly wrongful conduct, systematic violation, high number of affected data subjects, long time period of the conducted infringement, category of affected data subjects (employee, naked women under the shower), serious consequences of the infringement (mental handicap with disease value), large number of recipients (publication on social networks), measures not taken to mitigate the damage, relevant criminal records, no collaboration in the proceedings, intentional behaviour (dolus), degree of responsibility, high economic benefit derived from the injury

Additional information:

1) Data Breach Notifications since 25 May 2018 until 30 November 2019:
   DBN that were lodged with the AT SA: 1359
   DBN that the AT SA received through the IMI and was CSA: 177

2) Initiatives for SMEs
   annual campaigns for awareness raising, presentations and lectures in front of various audiences, providing guidance material and FAQs on our website, attending conferences, adoption of DPIA lists