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

ANSWERS FROM THE GREEK 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?
   We believe that the Commission should consider issuing an adequacy decision regarding major international organizations (such as but not limited to, for example the UN and its agencies) that transfer personal data on a regular basis in the framework of providing humanitarian assistance.

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 HDPA has not been identified as a LSA in one case so far. 6 cases in the case register have been initiated by the HDPA (in order to identify the LSA). There are 165 cases (in IMI case register), 17 draft decisions and 11 final decisions where the HDPA is a CSA.

b. Did you encounter any problems/obstacles in your cooperation with the lead/concerned DPA? If yes, please describe them
   In a couple of cases, there was no feedback from the LSA, after a long period of time.

c. How would you remedy these problems?
We try communicating the LSA through informal contacts.

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. A draft decision is considered to be the formal initial decision taken by the HDPA (by the appropriate body, as the HDPA can act as a college of commissioners in plenary or in a smaller group/section or in some cases by the President - please see question 2), after hearing the controller/processor.

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)?
We used the derogation on a couple of cases.

f. Is the OSS living up to its expectations? If not, what would you identify as its shortcomings? How can they be remedied?
We feel that differences in MSs administrative laws make the OSS less effective. Although, as stated, the HDPA is involved in a small number of OSS operations, we wish for a greater harmonization.

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?
Yes.

c. Is this tool effectively facilitating your work? If yes, how? If not, why?
Yes, it makes handling cases and investigations easier.

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?
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

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"?
N/A

e. Were there any issues concerning the translations and/or any other relevant information?
N/A

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?
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

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?
IMI is suitable for message exchange, but we consider that IMI is not a complete Cross Border Case handling System. The fact that most SAs use more systems to keep track of IMI operations (e.g. Excel files) indicates that there is a need to plan a new system. An alternative would be to find a solution to add case handling and overviewing functionality to IMI. For SAs lacking resources, constantly monitoring IMI and updating different 'systems' (xls – internal IT) is difficult, time consuming and a low priority for the management.
SAs lacking resources prioritize cases, leaving the initiative to other SAs.

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 figures requested are as follows: 39 (for 2016), 35 (for 2017), 33 (for 2018), 33 (2019), 46 (2020). Please note that we are referring to the number of **actual employees** per year and **not to the number of filled positions**.*

   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.

   For 2016 it was 2,068,000€; 2,380,000€ for 2017, 2,541,000€ for 2018, 2,849,000€ for 2019 and 3,101,000€ for 2020.

   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 HDPA is also competent for enforcing: a) most of the ePrivacy provisions (law 3471/2006 as amended), b) the national law 4624/2019 (that implements Directive 680/2016 and art. 9A of the Constitution of the Hellenic Republic - the article on Data Protection) and provides that the HDPA is competent to supervise every national and transnational processing operation, with limited exceptions for national security. We estimate that approximately 1/3 of complaints and cases arise from these sectors. Moreover, the Hellenic DPA is the competent data protection supervisory authority that is entrusted with the supervision of the Europol National Unit, and the national databases / systems of N. SIS II, VIS, Eurodac, CIS and PNR according to the relative European Regulations and Decisions (in the case of PNR, this is the national law 4579/2018 which transposed Directive (EU) 2016/681).

   d. How would you assess the resources from your DPA from a human, financial and technical point of view? *The resources at the moment are still insufficient. The estimation of the HDPA, as recently reported to the National Parliament, is that for the Authority to perform its tasks, the number of employees must increase to 108.*

   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, the HDPA is not adequately staffed. Right now 2 employees are assigned with all IMI handling operations and 3 more users can act as "backup" in selected IMI operations. These employees are not dedicated to IMI. We estimate that IMI operations account to an equivalent of 2 person days per month. Although the HDPA has not been identified as a LSA in any OSS case so far, we understand that given the high number of IMI notifications and procedures, there is a moderate risk of 'neglecting' a case, or of leaving the initiative to the rest of the SAs.

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?

   ***1569** Complaints have been received from 25-05-2018 to 31-12-2019.*
   The HDPA has issued four standard complaint forms, where every piece of information that is necessary for a complaint's investigation is specifically noted. Complaints that are filed without the necessary information are rejected (or the HDPA can use them for ex-officio investigations). Necessary

information contains: Details of the data subject, information on the data controller/processor, the actual complaint, in the case of a Data Subject Request information proving when and how the request was made and all accompanying documents.

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

Warning, Reprimand, Order to the controller/processor to bring processing operations into compliance with the provisions of the Regulation, Temporary limitation of processing, Administrative fine.

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

Although there is no formal "amicable settlement" provision in our legislation, in practice we use of process of "amicably" handling complaints. We envisage the term amicable as follows: When the infringement is a minor one and the data subject is satisfied, there is no need for the HDPA to exercise its corrective power. This practice allows us to process a large number of complaints. Under the recently approved GDPR implementing law (law 4624/2019) the President of the SA can also exercise some of the powers of art. 58 but this needs to be provided in HDPA's Rules of Procedure. Right now the HDPA is considering several options that would facilitate amicable resolution of complaints. It is also worthwhile mentioning that for the proper functioning of the GDPR implementing law in Greece two legal acts must be amended: a) the Rules of Procedure governing the operation of the HDPA, including case handling procedures and b) the Presidential Decree (on the internal structure of the HDPA). The procedure of amicable settlement can (probably) be defined within the Rules of Procedure.

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

16 fines have been imposed since May 2018 (total amount: 1,397,000€). 6 decisions were issued based on GDPR provisions (total amount: 715,000€). The rest of the fines were issued for ePrivacy infringements, or for infringements before May 25, 2018.
Examples:

Decision 26/2019

The HDPA conducted an ex-officio investigation, following a complaint that the employees of the company were required to provide consent to the processing of their personal data. The choice of consent as the legal basis was inappropriate, as the processing of personal data was intended to carry out acts directly linked to the performance of employment contracts, compliance with a legal obligation to which the controller is subject and the smooth and effective operation of the company, as its legitimate interest. The company gave employees the false impression that it was processing their personal data under the legal basis of consent. The company transferred its compliance obligations to its employees by asking them to sign a statement.
Fine amount: 150,000€.

Decision 31/2019

The Hellenic DPA has received complaints from telephony subscribers of the Hellenic Telecommunications Organization ('OTE') who, although registered in the OTE's do-not-call register (according to Article 11 of Law 3471/2006), they received unsolicited calls from third companies for the promotion of products and services.
The investigation of the case showed that those subscribers had submitted a portability request for the transfer of their subscription to another provider. As a consequence, OTE deleted their entries from the do-not-call register. However, when those subscribers cancelled their portability request, there was no proper procedure to cancel their removal from the register. Subscribers were listed as registrants in the internal system of the provider's customer service, but their telephone numbers were not included in the register sent by OTE to the advertisers, as the two systems, due to the error in their interconnection, did not have the same content.
Fine amount: 200,000€.

Decision 34/2019

The Hellenic DPA has received complaints from recipients of advertising messages from OTE concerning their lack of ability to unsubscribe from the list of recipients of advertising messages. In the course of the examination of the complaints it emerged that from 2013 onwards, due to a technical error, the removal from the lists of recipients of advertising messages did not operate for those recipients who used the "unsubscribe" link. OTE did not have the appropriate organisational measure, i.e. a defined procedure by which it could detect that the data subject's right to object could not be satisfied. Subsequently, OTE removed around 8.000 persons from the addressees of the messages, who had unsuccessfully attempted to withdraw from 2013 onwards.
Fine amount: 200,000€.

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

In our decisions we have practically considered all parameters of art. 83.2.

Examples:

Decision 26/2019

Aggravating factors: Nature, gravity and duration of the infringement: No evidence of compliance from the data controller, employees are considered as vulnerable data subjects, selection of a proper legal basis for the specific case doesn't pose a new legal issue, duration of the violation is from 25/5 until issuing the decision, number (485) of employees. Intentional character of the infringement. Although the data controller stated its intention to comply, no evidence of actions to mitigate the damage were presented. The infringement became known to the supervisory authority, after a complaint by a third party. Annual turnover is 41,936,426€.
Mitigating factors: No material damage to employees. No previous violations. Intention to comply. No special categories of data. No financial gain of the data controller.

Decision 31/2019

Aggravating factors: Duration of the violation is longer than three years. Around 16,000 data subjects were affected. As a result of the violation, data subjects were deprived of their -provided by law- right and kept being annoyed by unsolicited calls. Data controller is a large telecom provider that should ensure a high level of data protection. Annual turnover is 2,887,600€. Relevant previous infringements of the data controller are taken into account (decisions 1/2015 -after a data breach- and 16/2018). The controller realised there was an infringement after having being contacted by the DPA.
Mitigating factors: Negligent character of the infringement. Data controller acted immediately after getting notified by the DPA on the infringement correcting its procedures and the related data, in good cooperation with the DPA.

Decision 34/2019

Aggravating factors: Violation started in 2013. Around 8,000 data subjects were affected. Data controller is a large telecom provider that should ensure a high level of data protection. Annual turnover is 2,887,600€. Relevant previous infringements of the data controller are taken into account (decision 1/2015 after a data breach).
Mitigating factors: Negligent character of the infringement. Data controller acted immediately after getting notified by the DPA on the infringement correcting its procedures and the related data, in good cooperation with the DPA.