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

ANSWERS FROM THE MALTESE 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 specific concerns were raised regarding adequacy decisions adopted under Directive 95/46.

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?

There is no information on any such developments.

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

The Maltese SA does not have any particular preference in relation to a third country or international organisation, which should be considered for an adequacy decision. Nevertheless, in the event of Brexit, we believe that given the strong ties that exist and will continue to exist between EU Member States and the UK, an adequacy decision should be considered from the moment that the UK becomes a third country.

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?
Our DPA was identified as LSA in 19 cases and as CSA in 146 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?)
Our National Law does not provide for the parties to be heard before a decision is issued thus the step which can be referred to as "draft decision" is not needed. The decisions issued by the Commissioner are final decisions. The parties are heard or asked to make submissions at the investigation stage.
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)?
In 2019 our DPA dealt with two cases where the complaints were lodged by complainants residing in Malta but were related to a data controller's single establishment in another Member State. The complaints were referred to the identified LSAs, that accepted to handle the cases by raising Article 61 procedures.
f. Is the OSS living up to its expectations? If not, what would you identify as its shortcomings? How can they be remedied?
We believe that so far the mechanism is functioning according to the expectations.

1.2. Mutual assistance – Article 61

a. Did you ever use this tool in the case of carrying out an investigation?
Our DPA uses Article 61 Voluntary Mutual Assistance, within the IMI System, in the course of the preliminary investigation. Our DPA may use this tool to verify whether the data controller's establishment within its territory may be considered as the main establishment or whether such main establishment is the one existing within the territory of the other Member State.
b. Did you ever use this tool in the case of monitoring the implementation of a measure imposed in another Member State?
Our DPA uses Article 61 Voluntary Mutual Assistance, within the IMI System, mostly but not only, to ask for relevant information and assistance regarding others Member State practices related to specific sectors or matter.
c. Is this tool effectively facilitating your work? If yes, how? If not, why?
Yes. It is facilitating our work to communicate with other DPAs simultaneously and without the exchange of a disproportionate number of emails.
d. Do you encounter any other problems preventing you from using this tool effectively? How could they be remedied? N/A

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?
Our DPA never used this tool so far

b. Did you ever use this tool in the case of monitoring the implementation/enforcement of a measure imposed in another Member State? N/A
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)?
The only draft decision submitted to the Board under Art 64(1) is the one related to the list of the processing operations subject to the requirement for a data protection impact assessment (Art 64(1a)
b. Did you ever submit any draft decision to the Board under Art 64(2)? N/A
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.
The Board's opinion related to the list mentioned in point 2.1.b was taken into account by our DPA and was adopted accordingly
d. Was the "communication of the draft decision" complete? Which documents were submitted as "additional information"?
Yes it was complete and no other documents were submitted as additional information
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?
Given the limited number of Board opinions directly affecting our DPA we do not have sufficient experience dealing with this specific tool in order to provide a valuable feedback.

2.2 Dispute resolution - Article 65 GDPR

a. Was this procedure used? If yes, what was your experience during the process?
Our DPA never used this procedure so far
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?
Our DPA never adopted any measure under urgency procedure so far

3. Exchange of information: Standardised communication

a. What is your experience with the standardised communication through the IMI system?

Our DPA is satisfied with the level of standardisation provided though the IMI 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.
      2016 = 10; 2017 = 10; 2018 = 11; 2019 = 13; 2020 = 15
   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 = 340.000; 2017 = 380.000; 2018 = 430.000; 2019 = 480.000; 2020 = 550.000
   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.
      As part of its regulatory functions, this Office is also responsible for the enforcement of the freedom of information legislation. In 2018, 22 complaints were received while in 2019 the complaints received to-date are 19. On average FOI case load amounts to 20% of the total case work. Our office is also responsible for the implementation and enforcement of the ePrivacy Directive.
   d. How would you assess the resources from your DPA from a human, financial and technical point of view?
      Considering the volume of work and additional tasks assigned to DPAs under the GDPR we are of the opinion that, in view of our resources, we have to prioritise our activities and mainly focus on national work such as complaints, enquiries and other requests from organisations and the public at large. This leaves very limited time and resources to take a more prominent and proactive role at European level.
   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?
      At the moment we have 1 resource dedicated to the consistency mechanism. However, this person is carrying out additional tasks over and above such duties.

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?
      In 2018, the Commissioner has investigated 76 data subject complaints while in 2019, to-date, the complaints received are 102. Each complaint is assessed on a case by case basis. A complaint may be submitted through a specific form available on our website. That said, complaints may also be lodged by post or by calling in person. The Commissioner's complaint handling procedure involves a preliminary assessment to establish the admissibility of the cases. In the event that the case is considered not admissible, it is not investigated.
   b. Which corrective powers did you use since May 2018?
      The corrective powers pursuant to Article 58 (a) (b) (c) (d) (e) (f) (i)
   c. Are you resolving any possible infringements of the Regulation with the help of so-called "amicable settlements"?
      Yes the DPA has started to consider this possibility.

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

29. This number includes fines imposed for personal data breaches handled as local cases (the data controller main establishment is within the Maltese territory and the case concerns only data subjects within the Malta territory) and local complaints. The causes of such breaches are: human error, hacking and phishing attacks. The fines imposed for the complaints are related to unlawful and excessive processing.

For cross-border complaints the fine imposed are 2 for the infringement of the right of access and right to object.

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

As attenuating circumstances this DPA takes into account the cooperation of the data controller during the investigation, while we consider aggravating circumstances the repetitiveness of the breach and serious impact on the data subjects.

f. National statistics on data breaches

During the period from 25th May 2018 until 6th December 2019, the Maltese SA received a total of 218 data breach notification.

g. National initiatives to give guidance to SMEs or any other specific support to the SMEs.

The Maltese SA has successfully applied for EU funds, under the Rights, Equality and Citizenship Programme, to implement a project which, in part, is specifically dedicated to assist SMEs in complying with their data protection obligations. To this effect, an online compliance tool will be developed and launched during an event that will be organised together with constituted bodies in Malta.

The agreement with the European Commission was signed on 2nd December 2019 and the project will run for 24 months.