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

ANSWERS FROM THE POLISH 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)?

   Apart from general inquiries regarding the adequacy decisions adopted under the 1995 Directive, the Polish DPA did not receive inquiries in which any particular concerns regarding one of the adopted adequacy decisions would be raised.

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?

   Apart from publicly available knowledge, the Polish DPA does not have any specific information on the developments of the data protection system of any of the countries/territories subject to an adequacy decision under the Directive.

3. In your view, should any third country or international organisation be considered by the Commission in view of a possi Given the progressive, very rapid development of technology, the need to adopt new SCCs and the great uncertainty about the possibility of continuing to apply currently adopted SCCs (we are still waiting for the judgment of the CJEU in case Schrems II), as well as problems that arise in practice when applying the derogations set out in Article 49 GDPR, in our opinion, one should strive to adopt as many new adequacy decisions as possible for various countries or territories, remembering about the need to take into account the assessment criteria indicated in art. 45 (2) GDPR. In the document of July 24 entitled "Communication from the Commission to the European Parliament and the Council. Data protection rules as a trust-enabler in the EU and beyond – taking stock", it has been underlined how important the subject decisions are, indicating at the same time that their adoption by the European Commission along with the steps taken by other countries, gives a possibility of potential "to create a network of countries where data can flow freely" (p. 12 of the document in question).

   Undoubtedly, the adoption of an adequacy decision in relation to India should be considered, also taking into account the reality of the worldwide data flow and the ongoing legislative work on data protection law in India. The adoption of an adequacy decision on Australia also remains to be considered. This possibility has already been pointed out in the past. In this respect, an opinion was even issued by the Working Party („Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000") stating that „data transfers to Australia could be regarded as adequate only if appropriate safeguards were introduced to meet the above mentioned concerns". It is also worth paying attention to the provision of art. 45 (1) GDPR, which explicitly indicates that adequacy decisions may also be adopted in relation to a specific territory. On January 1, 2020, the California Consumer Privacy Act will enter into force. Perhaps this will create the basis to start, if not the work, then at least analyses on the possibility of adopting an adequacy decision on California.ble adequacy decision?

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?
329 as a CSA; 5 as a LSA (State of play: 30 November 2019)

b. Did you encounter any problems/obstacles in your cooperation with the lead/concerned DPA? If yes, please describe them
There is no rule as to what constitutes a 'relevant information' that should be exchanged between the LSA and CSAs. As a CSA we encounter situations where the LSA accepts to handle the case and does not communicate anything to the CSAs until it issues a draft decision. The CSAs which are not informed about the proceeding are then given a limited time to comment on the draft. Moreover, limited amount of attachments is presented, thus the CSAs are not able to verify the accuracy of the decision and whether the parties had a possibility to be heard before issuing the draft decision.
The interpretation of what constitutes a 'draft decision' under the GDPR is also problematic. Finally, there also exist different procedural rules and approaches towards handling of cases, and there is no unified procedure that will be applicable to cross-border (OSS) cases.

c. How would you remedy these problems?
Introduction of the unified procedural guidelines for all SAs handling the cross-border cases seems to be inevitable as more and more conflicts relating to the way cross-border cases are handled might arise.

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?)
Polish national administrative procedure does not identify the step referred to as the draft decision, however when the Polish SA gathers sufficient material to issue a decision it informs the parties that the material has been gathered and the decision will be issued. The parties, after reception of this

information, have some time to come and see all the evidence gathered and to introduce comments. Then the decision is issued.

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)?
Our SA has not been identified as locally competent to handle any cross-border case, however, we have agreed that the Czech SA should handle one of the cases for which the Polish SA is a LSA - locally.

f. Is the OSS living up to its expectations? If not, what would you identify as its shortcomings? How can they be remedied?
The differences in national procedural rules make the OSS mechanism only a tool to exchange information and not really to cooperate with each other in order to reach a consensus as of how the decision should look like. Some of the authorities have a possibility and use an amicable settlement to the cross-border cases, other have to issue a decision and the fact that the SA is willing to solve the case amicably is not communicated to the CSAs involved.
Thus, we would propose to unify the procedural aspects of carrying the cross-border proceedings.

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? **Not yet.**
c. Is this tool effectively facilitating your work? If yes, how? If not, why? **Yes.**
This tool facilitates the exchange of information between the SAs. This information relates to findings, legal background and practice of one or more SAs.
d. Do you encounter any other problems preventing you from using this tool effectively? How could they be remedied?
As soon as the feature in the IMI allowing for the communication with more than one SA has been introduced, the problem of lack of possibility to communicate with several SAs is no longer valid.

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? **Not applicable.**
d. Did you encounter any problems (e.g. of administrative nature) in the use of this tool? How could they be remedied?
As our national legislation allows for the employees of other SAs to be involved in the joint operations, some SAs seems to have encountered problems of the administrative nature as their national rules do not foresee such a possibility. The Spanish SA is working on the empowering of the use of art. 62 to any SA through the procedure that would not involve signing of the MoA.

2. Consistency mechanism

2.1 Opinion - Article 64 GDPR

a. Did you ever submit any draft decision to the Board under Art 64(1)? **No.**

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. **Not applicable.**
d. Was the "communication of the draft decision" complete? Which documents were submitted as "additional information"? **Not applicable.**
e. Were there any issues concerning the translations and/or any other relevant information? **Not applicable.**
f. Does that tool fulfil its function, namely to ensure a consistent interpretation of the GDPR? **Not applicable.**

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? **Not applicable.**
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? **Not applicable.**

2.3 Urgency Procedure – Article 66

d. 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?

The Polish SA finds this tool very useful and handy, however, some of the features might be ameliorated.

For example, art. 61 VMA requests require these requests to be made through already created Case Register. This means that any question to be asked has to be created from the case, even if it does not relate to any particular case. Moreover, there are many fields to be filed which are not strictly necessary while creating art. 61 and 56 procedures.

Nevertheless, this tool is a convenient and quick way to exchange information and it should be maintained.

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.
      1) the state as of 31 December, 2016 – 151.525 full-time (155 persons);
      2) the state as of 31 December, 2017 – 158.65 full-time (162 persons);
      3) the state as of 31 December, 2018 – 232.25 full-time (235 persons);
      4) the state as of 30 November, 2019 – 235.55 full-time (238 persons);
      5) forecast for 2020 – 260 full-time.
   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.
      1) 2016 – 19,287,000 PLN
      2) 2017 – 20,860,000 PLN
      3) 2018 – 21,006,00 PLN
      4) 2019 – 31,985,000 PLN
      5) forecast for 2020 – 40,111,000 PLN
   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 President of the Personal Data Protection Office is the competent data protection authority within the meaning of the GDPR. He is also, inter alia, a supervisory authority within the meaning of Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 and within the meaning of the Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016.
      It should also be noted that pursuant to the Act of 9 April 2010 on access to business information and exchange of business data, the President of the Office provides opinions on the data management regulations adopted by the management board of the business information office.
   d. How would you assess the resources from your DPA from a human, financial and technical point of view?
      In accordance with the 2019 Budget Act of 16 January 2019, a budget of PLN 31,985,000 was allocated to the Polish DPA. Notably, taking into account the staffing, technical and financial needs, the Office requested a budget of PLN 35,660,000 for 2019. Currently, given the amount of the allocated budget, the number of full-time employees is 235.55 (i.e. 238 employees) - as of 30 November 2019.
   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?
      In the Polish DPA, 11 people work on issues related to the cooperation and compliance mechanism. However, this number is insufficient.

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?
Since May 2018, 12 387 complaints have been received by the Polish DPA (as of 14 October 2019). Notably, any correspondence received by the Office which meets the requirements of the Act of 14 June 1960 the Code of Administrative Procedure shall be treated as a complaint and handled as a complaint. A complaint may be lodged:
1) in traditional form, i.e. in person at the seat of the President of the Office;
2) by post to the address of the Office;
3) through the Electronic Mailbox of the President of the Office.

b. Which corrective powers did you use since May 2018?
From May 2018 the Polish DPA used the following corrective powers in accordance with Article 58(2) of the GDPR:
1) to issue reprimands to a controller or a processor where processing operations have infringed provisions of the GDPR;
2) to order the controller or the processor to comply with the data subject's requests;
3) to order the controller or processor to bring processing operations into compliance with the provisions of the GDPR;
4) to order the controller to communicate a personal data breach to the data subject;
5) to order the erasure of personal data pursuant to Articles 17 of the GDPR.

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.
Since May, 2018 the President of the Personal Data Protection Office has imposed the following financial fines:

1) **the decision of 15 March 2019, imposing the first administrative fine in the amount of over PLN 943 000 (ca. €220 000) for the failure to fulfil the information obligation;**
2) **the decision of 25 April 2019, imposing a fine of over PLN 55 750 on the Lower Silesia Football association for infringement consisting in the publication of too wide a range of personal data of the judges who have been granted judicial licenses;**
3) **the decision of 10 September 2019, imposing a fine of an amount higher than PLN 2.8 million (ca. €645 000) on Morele.net for non-compliance with the required technical means of data protection, inter alia, the principle of confidentiality, as set out in Article 5 (1)(f) of the GDPR;**
4) **the decision of 16 October 2019, imposing an administrative fine of over PLN 201 000 ClickQuickNow sp. z o.o. for, inter alia, obstructing the exercise of the right to withdraw consent to the processing of personal data;**
5) **the decision of 18 October 2019, imposing the first administrative fine of PLN 40 000 on a public entity for failure to comply with the GDPR. The reason for imposing the fine was that the mayor of the city did not conclude a personal data processing agreement with the entities to which he transferred data;**
6) **a decision imposing a fine of PLN 2 000 on the housing community; the entity processing personal data with the use of video surveillance was not able to properly manage the surveillance in the scope of making available video surveillance recordings, as well as keeping record of the recordings made available;**
7) **a decision imposing a fine of PLN 8 000 on the company which managed the property for the processing of video surveillance data without entering into personal data processing**

entrustment agreement. Moreover, the company also failed to implement organizational and technical measures to ensure control over disclosed personal data coming from video surveillance;

8) **a decision imposing a fine of PLN 30 000 on a company dealing with the protection of property and persons; in its case, the supervisory authority stated that not all employees of the company having access to the video surveillance data had appropriate authorisations. Therefore, the company did not exercise control over the data processing, in particular by specifying in the authorisations the purpose, scope and manner of data processing by a particular person.**

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

1) <u>the decision of 15 March 2019</u> – despite being aware of the obligation to inform data subjects on their data being processed, the controller failed to do so, as well as to perform any activities aiming at remedying the infringement and mitigating its possible adverse effects;

2) <u>the decision of 25 April 2019</u> – good cooperation of the controller with the supervisory authority and the lack of evidence towards any damages to the data subjects whose data were disclosed, were the crucial attenuating circumstances taken into account in this case;

3) <u>the decision of 10 September 2019</u> – attenuating circumstances consisted in this case of e.g. the fact that the entity took actions towards remedying the infringement, good level of cooperation with the supervisory authority as well as the fact that the company had no previous history of data protection law infringements;

4) <u>the decision of 16 October 2019</u> – The President of the Personal Data Protection Office did not recognize any attenuating circumstances that might had been of influence on the final size of the fine. He concluded that the actions taken by the company were purposeful since sending contradictory announcements to the data subject interested in withdrawing his/her consent resulted in the fact that the consent withdrawal was not effective. This way the company hindered the possibility or even made it impossible for the data subjects to exercise their rights;

5) <u>the decision of 18 October 2019</u> – despite the fact that the violations of the data protection law were revealed in the course of the proceedings, they were not remedied by the controller nor the controller did implement solutions with a view to counteract future breaches. Also the controller did not cooperate with the supervisory authority. The President of the Personal Data Protection Office concluded that in this particular case there were no attenuating circumstances that might contribute to reducing the fine.

7. Additional questions

1) National statistics on data breaches:

From May 2018 to 30 November 2019 the Polish DPA received 7 957 data breach notifications.

2) National initiatives to give guidance to SMEs or any other specific support to the SMEs:

The Personal Data Protection Office in Poland constantly undertakes activities aimed at raising the awareness of, among others, entrepreneurs about the use of the GDPR. This takes place on many levels, including educational and informational activities. However, it is a long-term process, the

effects of which are not always immediately visible. Nevertheless, we systematically expand our activity, taking into account the needs of various environments.

Entrepreneurs can take advantage of many activities supporting them as data controller or processor. They have at their disposal, for example, the Office's infoline and the website www.uodo.gov.pl, through which they can keep up to date with both information on the latest positions and communications of the President of the Office and have access to the database of administrative decisions, which constitute a valuable source of practical knowledge about the principles of using the GDPR. Moreover, the website is constantly enriched with thematic studies in which entrepreneurs will find many guidelines of the President of the Office on the application of the GDPR (e.g. in the form of manuals).

In parallel to these activities, the Office develops cooperation with data protection officers. After last year's trainings, this year we have launched a special hotline and a thematic newsletter (used by more than 6 000 subscribers).

In addition, the Office monitors the legislative process and expresses opinions on the compliance of the draft regulations with the data protection law. In this way, we also pay attention to the role of the law design process.