

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

*PLEASE SEE THE ANSWERS TO FOLLOWING QUESTIONS FROM **DATA STATE INSPECTORATE OF LATVIA** (HEREINAFTER – THE INSPECTORATE)*

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)?

*The Inspectorate has not received this kind of specific questions.*

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?

*The Inspectorate does not have such information at the moment.*

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

*The Inspectorate does not have such information at the moment. However considering the public available Information at the home page of the Ministry of Economics of Latvia on its annual report, 2018 on development of export target markets (including distant markets), the main cooperation markets should be focused on USA, Japan, China, South Korea, Belarus, Regions of Russia. It might be considered that these countries might be relevant for possible adequacy decisions.*

## 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, joint 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, the Inspectorate has been involved in OSS cases since May 2018. Since May 2018 till now the Inspectorate has been involved in 106 OSS cases.*

b. Did you encounter any problems/obstacles in your cooperation with the lead/concerned DPA? If yes, please describe them

*Dealing with LSA or CSA in OSS cases, the Inspectorate has not encountered any significant problems.*

- 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?)

*The concept of 'draft decision' does not appear in our national administrative procedure, applicable on national investigation cases. “Draft decision” is new tool for the Inspectorate. Consequently, the definition of draft decision and its role in the cases must still be clearly understood by the Inspectorate in order to be properly applied in OSS cases.*

*Also, the Inspectorate would like to note, that according to national legislation, the decision of case should be made immediately after case hearing but not later than within five days, whereas the deadline of draft decision is longer. A solution to this issue is currently being sought.*

*Additionally, we inform, that in accordance with our national administrative procedure all parties in case must be heard. It means that before the draft decision has been made, all parties shall be given an opportunity to be heard.*

- 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)?

*Inspectorate currently has no experiences on the number of such cases under Article 56(2). In the view of the Inspectorate, this question concerns the interpretation of GDPR Article 56 (2) in which the Inspectorate lacks practical experience. However there were case where Inspectorate was considering to use this “local case” procedure. The Inspectorate would appreciate the views and practices of other supervisory authorities on this issue.*

- f. Is the OSS living up to its expectations? If not, what would you identify as its shortcomings? How can they be remedied?

*The OSS mechanism is a useful and necessary tool in the context of cross-border data protection supervision, especially in view of the increasing number of cross-border data processing. In the view of the Inspectorate, as a result of practical application, OSS procedure will only evolve. Inspectorate staff still face some technical difficulties in using IMI system, but increasing the Inspectorate's capacity, including the number of staff that could deal with OSS cases, could eliminate these problems and address OSS cases more effectively.*

### 1.2. Mutual assistance – Article 61

- a. Did you ever use this tool in the case of carrying out an investigation?

*Yes, the Inspectorate has used this tool once.*

- b. Did you ever use this tool in the case of monitoring the implementation of a measure imposed in another Member State?

*No, the Inspectorate did not used this tool in such case.*

- c. Is this tool effectively facilitating your work? If yes, how? If not, why?

*This tool is useful when the Inspectorate encounters a situation where there are reasonable doubts on case proceeding. This tool allows to use the experience of other countries in our work.*

*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, the Inspectorate has not used this tool yet.*
- b. Did you ever use this tool in the case of monitoring the implementation/enforcement of a measure imposed in another Member State?  
-
- 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?  
-

## 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, the Inspectorate has submitted draft decision to the Board under Art 64(1) a).*
- b. Did you ever submit any draft decision to the Board under Art 64(2)?  
*No, the Inspectorate has not submitted such draft decision.*
- c. Did you have any problems by complying with the obligations under Article 64(7) GDPR, i.e. taking utmost account of opinion of the EDPB? If so please describe them.  
-
- d. Was the “communication of the draft decision” complete? Which documents were submitted as “additional information”?  
-
- e. Were there any issues concerning the translations and/or any other relevant information?  
-
- f. Does that tool fulfil its function, namely, to ensure a consistent interpretation of the GDPR?  
*In generally yes. However as Inspectorate has not gained diversified experience on the application of this Article, it is to be expected to provide detailed comments in the future.*

### 2.2 Dispute resolution - Article 65 GDPR

- a. Was this procedure used? If yes, what was your experience during the process?  
*The Inspectorate has not used this procedure yet.*
- 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?  
*The Inspectorate has not used this procedure yet.*

## 3. Exchange of information: Standardised communication

- a. What is your experience with the standardised communication through the IMI system?  
*So far, the Inspectorate has not encountered significant communication problems in the IMI system that could interfere with investigation procedures. However, the Inspectorate is aware of the need and is currently working on developing the Inspectorate's internal procedures on handling of IMI cases.*

#### **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?

#### **4. 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- average 21*

*2017- average 22*

*2018- average 20*

*2019- average 20*

*The Inspectorate informs that there are 25 approved positions on the staff in 2019. In 2020 is expected that number of the staff will increase because of the approved additional budget for the Inspectorate.*

- 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.

*2016-619 604 EUR*

*2017-690140 EUR*

*2018-782894 EUR*

*2019-640998 EUR*

*2020- to be expected 1 218 978 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.

- *promotes public awareness on data protection;*
- *advise national parliaments, governments and other institutions and bodies, in accordance with the laws of the Member States, of legislative and administrative measures relating to the protection of the rights and freedoms of natural persons with regard to processing;*
- *monitor relevant developments as far as they affect the protection of personal data, and in particular the development of information and communication technologies and commercial practices;*
- *perform any other tasks related to the protection of personal data;*
- *monitor the compliance of data processing with the requirements of regulatory enactments, also in cases where the controller is prohibited by law from providing information to the data subject and has received a relevant application from the data subject;*
- *contribute to the effectiveness of data protection within its competence, provide recommendations to the Saeima, the Cabinet of Ministers, local governments and other institutions regarding the issuance or amendment of legal acts, as well as participate in drafting of regulatory enactments and development planning documents and provide opinions on draft regulatory enactments and development planning documents prepared by other institutions;*
- *co-operate with foreign data protection, information transparency and access control authorities and prohibition of commercial communication;*

- *represent the Republic of Latvia in international organizations and activities in the field of data protection;*
- *conducts research, analyzes the situation, makes recommendations and opinions, as well as informs the public on current issues in the areas of its competence;*
- *supervise the processing of personal data by the Passenger Information Unit in accordance with the requirements specified in regulatory enactments;*
- *oversees the Law on Extrajudicial Debt Recovery with regard to the protection of personal data;*
- *consider a complaint by a debt recovery service provider for refusal to correct inaccurate, incomplete or false information contained in the debt history database;*
- *compile reports of the Security Incident Prevention Authority regarding the processing of personal data carried out in the previous year;*
- *an application regarding the necessity to perform the verification regarding observance of the rights of the data subject specified in the Law of the Schengen Information System, if the data subject or his or her authorized person is refused to provide the requested information;*
- *impose an administrative penalty for violating the prohibition of commercial communication;*
- *compilation of statistical information on requests from institutions to receive retained data and on issuance of such data;*
- *registration of personal data breaches in the field of electronic communications;*
- *Authorization of the designated coding method to be used by the chief processor in the genome database;*
- *processing complaints and deciding on the collection of health records and genealogical data, coding and decoding of tissue samples, DNA profiles, health records and genealogical data, and processing of tissue samples, DNA profiles, health records and genealogical data;*
- *providing an opinion that the genome database provides the processing of personal data in accordance with the requirements of the regulatory enactments regarding the protection of personal data, including mandatory technical and organizational requirements for personal data processing systems;*
- *monitoring the operation of the commission for the destruction of personal data, tissue samples, DNA profiles and health records of the gene donor;*
- *agrees that the credit bureau may, on the basis of a written agreement, entrust another person with the activities necessary to ensure the performance of the licensed credit bureau activities specified in Article 7 of the Credit Information Bureau Act;*
- *publishing and updating information on a credit bureau on its website;*
- *making a decision to issue, suspend, renew or revoke a license to the Credit Information Office;*
- *publish a list of experts who can audit the credit information office;*
- *give an opinion to a person who wishes to become a shareholder of a credit bureau with at least five percent of the share capital, council or board member of a credit bureau, whether it meets the requirements of these regulations for a shareholder, council or board member;*
- *cooperate with the supervisory authorities of the Member States of the European Union and the European Data Protection Supervisor by exchanging information, assisting each other in carrying out audits and inspections in Eurodac;*
- *conduct an audit of Eurodac regarding the processing of personal data in accordance with Article 33 (2) of the Eurodac Regulation, including randomly analyzing substantiated electronic requests;*
- *cooperate (exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties in the interpretation or application of the SIS II Regulation, analyze*

*problems arising from independent monitoring or exercise of data subjects' rights, make coordinated proposals seeking common solutions to all problems; and assist, where necessary, in the identification of data protection rights) with the supervisory authorities of the Member States of the European Union and the European Data Protection Supervisor in order to ensure coordinated supervision of SIS II;*

- *audit the data processing operations performed by N.SIS II of Latvia in accordance with international auditing standards;*

- *provide assistance to, and advise to, an interested party regarding the protection of the rights of a person concerning the rectification or erasure of data concerning him in the VIS, in accordance with the VIS Regulation [3];*

- *carry out audits of data processing operations within the VIS in accordance with the relevant international auditing standards;*

- *cooperate (exchange relevant information, assist one another in carrying out audits and inspections, examine difficulties in the interpretation or application of the VIS Regulation, analyze problems arising from independent monitoring or the exercise of data subjects' rights, formulate coherent proposals seeking common solutions to all problems; data protection rights) with the supervisory authorities of the Member States of the European Union and the European Data Protection Supervisor to ensure coordinated supervision of the VIS;*

- *shall, at the request of another Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, furnish information on its national law and administrative practice in the field of data protection in accordance with its national law and for the sole purpose of protecting in respect of certain automatic processing operations carried out in its territory, but excluding personal data processed;*

- *consider the request of the data subject regarding the processing of his or her personal data or the verification of the processing thereof in the cases specified in the Law On Processing of Personal Data of Criminal and Administrative Violations;*

- *give an opinion on the impact of the processing of personal data on data protection in the case specified in the Law On Processing of Personal Data in Criminal and Administrative Violations;*

- *registration of personal data protection breaches specified in the Law on Processing of Personal Data of Individuals in Criminal and Administrative Violations;*

- *shall carry out the administrative violation proceedings in accordance with the violations referred to in Section 32 of the Law On Processing of Personal Data in Criminal and Administrative Violation Proceedings by the Data State Inspectorate.*

- *examines complaints about the actions of the Competition Council restricting the right of a natural person as a data subject to access information on whether or not the personal data of a particular person are being processed until the information necessary for making a decision is obtained;*

- *perform other tasks provided for in regulatory enactments.*

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

*The Inspectorate lacks resources in terms of staff, financial and technical resources. Given that the number of duties resulting from the direct application of the Regulation has increased, the Inspectorate needs additional resources to effectively implement its obligations under the Regulation. This also includes strengthening the Inspectorate's technical capacity especially in the view of investigation processes.*

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?

*Currently, the Inspectorate lacks the human resources to provide effective cooperation and consistency mechanism. At the moment there are 2 Divisions (Division of European Union and international cooperation and Division of Supervision and personal data processing) involved working on the issues devoted to the cooperation and consistency mechanism. There are 8 employees working at the moment in these divisions together, however the number of exact persons involved in specific cases are designated on case by case basis. Especially the lack of capacity as regards to IT experts is to be mentioned.*

## **5. 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?

*The Inspectorate received 2232 complaints since May 2018. The complaint is considered to be an application of person on his personal data processing.*

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

*In the processes of investigation, the Inspectorate applied corrective measures which is set out in Article 58(2) (a) – issued warnings, (b) – issued reprimands, (c) ordered the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation, (d) - ordered the controller or processor to bring processing operations into compliance with the provisions of GDPR, (e) - ordered the controller to communicate a personal data breach to the data subject, (g) ordered the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19, (i) imposed an administrative fines.*

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

*The Inspectorate informs that in accordance with the Administrative Procedure Law (the provisions of this Law shall be applied by the Inspectorate in considering applications and complaints), the possibilities of concluding a settlement may be examined. For example, Article 80.1. of Administrative Procedure Law determines that when considering an application to challenge an administrative act, the institution shall consider the possibility of concluding an amicable settlement (administrative contract) before taking a decision. If the institution considers the settlement to be possible, it shall inform the individual of the settlement procedure and the possible terms of the settlement, in order to allow him to express his views on the settlement. The Inspectorate adds that, according to Administrative Procedure Law, mentioned settlement could be concluded between the Inspectorate and the controller and not between the controller and the data subject. However, the Inspectorate informs, that the Inspectorate has not experience so far in the process of concluding an amicable settlement.*

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

*From 2018 the Inspectorate imposed 19 fines (which does not include warnings). (For example, 2000 EUR – unlawful video surveillance, 2000 EUR- failure to provide information to the data subject, 7000 EUR- failure to provide information to the data subject, failure to cooperate with the supervisory authority).*

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

*Imposing the fine, the Inspectorate takes into account first of all provisions of Article 83, Point 2 of GDPR, additionally - the attenuating and aggravating circumstances provided in national administrative laws. In Latvian Administrative Violations Code as mitigating circumstances have been provided: 1) if the person at fault has frankly regretted what he or she has done; 2) if the person at fault has eliminated the harmful consequences of the violation, voluntarily compensated the loss or eliminated the damage committed; 3) if the violation was committed under the influence of strong mental agitation or due to serious personal or family circumstances; 4) if the violation was committed by a minor; 5) if the violation was committed by a*

woman who is pregnant or a woman who has a child aged up to 1 year; and 6) if a person at fault has voluntarily applied prior to disclosing of the committed violation. As aggravating circumstances have been established: 1) if the unlawful action is continued, regardless of an authorised persons' request to cease it; 2) if a similar violation, regarding which a person had been already punished, has been committed repeatedly within a year; if the administrative violation has been committed by a person who has previously committed an offence; 3) if a minor has been involved in the committing of a violation; 4) if the violation has been committed by a group of persons; 5) if the violation has been committed during a natural disaster or other emergency circumstances; 6) if the violation has been committed under the influence of alcoholic beverages, narcotic or other intoxicating substances. Depending on the nature of the violation, the institution (official), which imposes administrative sanction, may decide not to consider circumstance as being liability aggravating. Additionally, the Inspectorate would like to mention, that there will be new administrative procedure law which will come into force from 1st July 2020. In this law there is also set out attenuating and aggravating circumstances, which are not much different from previous ones.

### **Additional questions**

We hereby send the additional requested Information on **data breach notifications**: in 2018 – 46, in 2019 – 107, total number – 153.

### **Additional information on specific initiatives for SMEs:**

Since 2018 Inspectorate participates as the Leading Authority in the European Commission's Project on "General Data Protection Regulation possibilities and responsibilities for small and medium-sized enterprises (SMEs); rights and risks for minors (DPSME)". The Aim of the Project is to improve the readiness of the small and medium-sized enterprises and to fulfill the requirements of the GDPR. Project's time frame is 24 months - 01.12.2018.-30.11.2020. In 2019, 10 seminars were organized in all regions of Latvia (Riga, Jelgava, Cesis, Jekabpils, Ventspils, Valmiera, Daugavpils, Liepaja, Ludza) and a final conference in Riga, November 26 on different topics for SMEs, where lecturers from Latvia and abroad shared their experiences. Within this phase, a recommendation - a Guide to Data Processing for Small and Medium-Sized Enterprises (<https://www.dvi.gov.lv/en/general/recommendation-celvedis-data-apstrade-small-and-modernem/>) was also developed. The next stage will be regional educational seminars (4-hour training workshops) and National competition for minors (aged 13 to 17) implemented during 2020.

Inspectorate participates also in a project of the European Commission - GDPR Compliance - Cloud Platform for Micro Enterprises as a partner for the Leading authority – Spanish Company. Time frame of the Project is 01.05.2018-31.10.2020 and aim is to develop a cloud platform and a handbook for micro enterprises in order to ensure the compliance with GDPR.

The most common way of providing and information is also Inspectorate's ability to provide a written answers to person's applications, on-the-spot consultations (on previous agreed time frame) and phone consultations. Any interested person (also SMEs) are welcomed to clarify an information on different questions on personal data protection.

*Additionally there are also different seminars, workshops, conferences organised in Latvia, where Inspectorate is invited to act as a speaker (also with relevant topics for SMEs). For example, on 29th May, 2019 the Forum “Digital Era” – (Data safety and GDPR Forum) was organised where also Inspectorate’s representatives were invited to speak.*