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

ANSWERS FROM THE LUXEMBOURGISH 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)?

The National Commission for Data Protection (CNPD) has not yet received any question about the substance of the adequacy decisions adopted under the 1995 Directive by a stakeholder. However, the CNPD handled information requests on the scope of some adequacy decisions, such as the ones concerning Canada and Japan (material scope) and the ones concerning Guernsey, Jersey and the Isle of Man (territorial scope, mostly in relation with Brexit issues).

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.

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

In the event that the UK leaves the EU, the CNPD takes the view that the UK should be considered by the Commission in view of a possible adequacy decision. Moreover, International Organisations such as United Nations agencies should be taken into account by the Commission for such assessment.

CHAPTER VII

The GDPR provided for one single set of data protection rules for the EU (by a Regulation) and one interlocutor for businesses and one interpretation of those rules. This "one law one interpretation" approach is embodied in the new cooperation mechanism and consistency mechanisms. In order to cooperate effectively and efficiently the GDPR equips the Data Protection Authorities (thereafter the DPA/DPAs) with certain powers and tools (like mutual assistance, join operations). Where a DPA intends to adopt a measure producing effects in more than Member State, the GDPR provides for consistency mechanism with the power to ask for opinions of the European Data Protection Board (EDPB) on the basis of Article 64(1) and (2) GDPR. In addition, in situations where the endeavour to reach consensus in the cases of one-stop shop (OSS) does not work (i.e. there is a dispute between the DPAs in specific cases), the EDPB is empowered to solve the dispute through the adoption of binding decisions.

In this context, the Commission finds it appropriate to request the views of the DPAs / EDPB on their first experiences on the application of the cooperation and consistency mechanisms. To this aim, the Commission established the list of questions below, in order to help the DPAs framing their input. It is understood, that the Commission is also interested in any comments the DPAs may have which goes beyond the answer to the questions and which concerns the application of the two above-mentioned mechanisms.

1. Cooperation Mechanism

1.1. OSS – Article 60

a. Has your DPA been involved in any OSS cases? If so, in how many cases since May 2018?

Yes, the CNPD counts 277 complaints which it received as lead supervisory authority, 26 complaints initiated as a concerned supervisory authority and 137 OSS cases where it declared itself as a concerned supervisory authority (status: 1st December 2019).

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

Since May 2018, the CNPD has encountered the following issues:

- ***As a concerned supervisory authority, the CNPD has noticed that in some cases, the presumed lead authority failed to act as such, by not providing any feedback in the article 56 procedure in IMI;***
- ***As a concerned supervisory authority, the CNPD has noticed that in some cases, the lead authority did not provide any follow-up to a specific case, even on request;***
- ***As a concerned supervisory authority, the CNPD has noticed that several lead authorities have resolved a specific case either by issuing a warning to the controller or by amicable settlement with the controller without any informal consultation with the CSA(s) or without issuing a draft decision;***
- ***As a lead supervisory authority, the CNPD has noticed that many cases that were sent to the CNPD were incomplete, contained untranslated joint documents or were not properly assessed [e.g. the data subject did not contact the controller before lodging a complaint, the topic of the complaint related to litigation (e.g. locked accounts, unpaid items, disputes between sellers and buyers, etc.) or consumer disputes rather than data protection issues];***
- ***As a lead supervisory authority, the CNPD has noticed that personal data of complainants have been shared systematically with every EU member state, including all German Länder, although the assessment of these cases revealed that these complaints only had a limited individual impact;***
- ***On a general note, the criteria for a supervisory authority to be considered as a concerned authority as per Article 4(22)b seems very vague in practice.***

c. How would you remedy these problems?

It is up to each supervisory authority to deal with every case with all due diligence.
However, as the assessment of a case varies from one Member state to another, the CNPD believes the above problems can only be remedied by issuing additional guidelines or by organizing further workshops between Member states.
Moreover, the provisions of the GDPR could be clarified on the following points:

- ***The consequences for a lead authority which does not act as such;***
- ***The exact meaning of "exchanging all relevant information", especially with regard to complaint handling;***
- ***The exact criteria of a local case as per Article 56(2) GDPR;***
- ***Further criteria to avoid that the GDPR is systematically instrumentalised in context of consumer disputes or to circumvent legal proceedings;***
- ***Clearer rules for a supervisory authority to be considered as a concerned authority, especially when it comes to cases that, although of cross-border nature, only have a limited individual impact.***

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?)
There are no specific provisions regarding the One-stop-shop mechanism in the Luxembourg act of 1st August 2018.
Decisions taken by the CNPD which are notified to the controller or which close a complaint are considered as per the Luxembourg national law as administrative decisions, which entails that they are binding and that the controller or the complainant can appeal against them. The rights of the defence and due process are respected. The controller can also present his comments on the draft decision as per Article 60.3 GDPR.

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)?
As a lead supervisory authority, the CNPD only had very few cases to be considered as local cases. These cases referred to data protection issues in the employment context.
As a concerned supervisory authority, the CNPD did not handle any case as a local case as per Article 56(2) GDPR.

Is the OSS living up to its expectations? If not, what would you identify as its shortcomings? How can they be remedied?
Generally, the CNPD believes that there are still substantial challenges to overcome because for the time being, too much time and too many resources are spent on minor cases. Mainly, the CNPD takes the view that cases, although of cross-border nature but with only limited individual impact should not need consultation with all CSA's as it adds unnecessary delays to rather simple matters.
Thus, Articles 56 and 60 GDPR should be modified in this respect in order to simplify the procedure regarding cases with only a limited individual impact.

1.2. Mutual assistance – Article 61

a. Did you ever use this tool in the case of carrying out an investigation?
Yes. During the assessment of specific cases, the CNPD has frequently used this tool either to ask for clarifications or additional information, to provide a follow-up, or to ask for support in the investigation on a specific topic. Furthermore, the CNPD has made use of this tool to ask general questions to one or several supervisory authorities on a principle matter, on best practices or on legal issues.

b. Did you ever use this tool in the case of monitoring the implementation of a measure imposed in another Member State?
No.

c. Is this tool effectively facilitating your work? If yes, how? If not, why?
Yes. Because it is a quick and effective way to communicate with another supervisory authority.

d. Do you encounter any other problems preventing you from using this tool effectively? How could they be remedied?
No, except from minor technical issues in IMI which are addressed by the Secretariat of the EDPB anyway, the CNPD does not encounter any problems in using the article 61 procedure.

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. There was no need yet for the CNPD to formally launch a joint operation as per article 62 GDPR.

b. Did you ever use this tool in the case of monitoring the implementation/enforcement of a measure imposed in another Member State?
No. As under question a), there was no need to do this.

c. Is it effectively facilitating your work? If yes, how? If not, why?
N/A – see question a.

d. Did you encounter any problems (e.g. of administrative nature) in the use of this tool? How could they be remedied?
As described under question a., the CNPD did not launch a formal joint operations procedure yet. The CNPD believes however, that local laws may cause confidentiality issues when it comes to sending staff members to other EU member states.

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 CNPD requested the opinion of the Board for the national list of processing operations for which a DPIA is required in Luxembourg as well as for draft criteria for accreditation of certification bodies.

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. The Luxembourg supervisory authority took account of the Boards' comments and made the requested changes.

d. Was the "communication of the draft decision" complete? Which documents were submitted as "additional information"?
In the case of draft criteria for accreditation of certification bodies, the CNPD submitted further documents such as a template for adopting requirements for accreditation of certification bodies, a "standard on assurance engagements" or an "international standard on quality control".

e. Were there any issues concerning the translations and/or any other relevant information?
No, as the CNPD submitted all documents in English language.

f. Does that tool fulfil its function, namely to ensure a consistent interpretation of the GDPR?
The CNPD believes that it is too early to tell. Until now, with the few cases at hand, the system seems to work fine.

2.2 Dispute resolution - Article 65 GDPR

a. Was this procedure used? If yes, what was your experience during the process?
No, the CNPD did not use this procedure yet.

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, the CNPD did not adopt any such measures yet. Furthermore, there are no specific provisions regarding the urgency procedure in the Luxembourg act of 1st August 2018.

3. Exchange of information: Standardised communication

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

The CNPD considers the IMI system to be very satisfying, although there is room for technical improvement. In any case, the CNPD regularly presents its observations to the IT User Subgroup, which deals with the technical issues of IMI. To mention one recent example, the limited character space in IMI is an important issue, as authorities are obliged to upload a word document as soon as the message exceeds 1000 characters, which, depending on the complexity of the case, is not much.

4. European Data Protection Board

a. Can you provide an indicative breakdown of the EDPB work according to the tasks listed in Article 70?

The CNPD participates in the work of each of the twelve Expert Subgroups (ESG) of the EDPB. Thereto, the CNPD either sends representatives to the regularly scheduled ESG meetings in Brussels or, where this is exceptionally not possible, asks to participate in those meetings via teleconference. The participation in each of the ESGs entails the contribution to the work of the Board (including via written comments).

In addition, the CNPD has been involved as co-rapporteur with regard to the following work items of the Board:

- ***Opinion on the interplay between the PSD2 and the GDPR;***
- ***Guidelines on blockchain ;***
- ***Use and retention of credit cards data;***
- ***Guidelines on connected assistants;***
- ***Opinion on the COM proposal for an e-evidence Regulation;***
- ***Opinion on the Japan Adequacy Decision;***
- ***Guidelines on data subject rights.***

Moreover, the CNPD has been acting as lead rapporteur on

- ***The Internal guidance to set up working procedures for delivering consistent opinions under national certification schemes as well as the***
- ***internal guidance on procedures for EDPB approval of criteria leading to the European Data Protection Seal.***

As to the allocation of internal resources, the CNPD has one employee who is working full-time on all matters relating to the EDPB and eight thematic experts working (approximatively 20% of the working time) on the matters related to the ESG they usually attend.

It follows from that indicative breakdown of the resources the CNPD dedicates to the contribution to the work of the Board, that they are mainly focused on the following tasks of the Board:

- ***to advise the Commission on any issue related to the protection of personal data in the Union (letter b of article 70 GDOR),***
- ***to examine any question covering the application of the GDPR and to issue guidelines, recommendations and best practices in order to encourage consistent application of the GDPR (letter e of article 70 GDPR) and***
- ***to contribute to the set-up of an internal procedure preparing the approval of the criteria of certification pursuant to article 42 (5) (letter o and p article 70 GDPR).***

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?

N/A

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: 19***
      - ***2017: 25***
      - ***2018: 38***
      - ***2019: 43***
      - ***2020: 48***

   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: 2.050.922 €***
      - ***2017: 2.499.348 €***
      - ***2018: 4.415.419 €***
      - ***2019: 5.442.416 €***
      - ***2020: 6.691.563 €***

   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.

Beyond the tasks the CNPD is entrusted with by the GDPR, the CNPD is competent to oversee processing of personal data in criminal and national security matters.

In addition, the CNPD is represented in the judicial control authority (created by article 40 of the Act of 1 August 2018 on the protection of individuals with regard to the processing of personal data in criminal and national security matters, transposing Directive EU 2016/680) which supervises the processing of personal data carried out by courts of the judicial order, including the public prosecutor, or the administrative order acting in their judicial capacities.

The CNPD is represented in the Commission on Access to Documents (created by article 9 of the law of 14 September 2018 on a transparent and open administration) which is tasked to ensure the right of access to administrative documents in the conditions foreseen by law.

The CNPD is also tasked with the supervision of the protection of privacy in the sector of electronic communications in accordance with the act of 30 May 2005 regarding the specific rules for the protection of privacy in the sector of electronic communications transposing the Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector and amended, although declared invalid by the EUCJ, by the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

Also, the CNDP is represented in the Commission of the national register, entrusted with the task to supervise the National Registry of Natural Persons.

Moreover, the CNPD is represented in several Supervision Coordination Groups tasked to supervise European large-scale IT systems:

- ***Customs Information System Supervision Coordination Group,***
- ***SIS II Supervision Coordination Group***
- ***Eurodac Supervision Coordination Group,***
- ***Visa Information System Supervision Coordination Group.***

Finally, the CNPD is represented in the Europol Joint Supervisory Body overseeing the lawfulness of personal data processing by Europol.

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

The Luxembourg government has provided the CNPD with all the requested resources, which has allowed the CNPD to grow constantly and substantially over the past five years.

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?

From an operational perspective, our annual budget has allowed us to attribute more resources to IMI complaint handling. For the time being, 8 staff members are handling (IMI and national) complaints. The cases are assigned to specialised experts (e-commerce, marketing, technical questions, etc.)

The controllers are mostly very reactive to the CNPD's requests.

The CNPD usually has a very good communication & personal contacts with the staff of several SA's which send complaints.

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?

- ***With regard to national cases, the CNPD has received 649 complaints since 25 May 2018 (status: 1st December 2019). With regard to statistics on data breaches, the CNPD has received 498 data breach notifications between 25 May 2018 and 1 December 2019.***
- ***The CNPD provides the data subjects with a complaint form. It lists all the information the CNPD needs to receive in order to thoroughly investigate. As such, the CNPD needs the correct identification of the data subject, the controller, the steps taken by the complainant prior to the complaint and enough information on the data processing and the alleged infringement. The CNPD can, of course, ask the complainant to provide additional information anytime.***
- ***With regard to cooperation cases, the CNPD has received 277 complaints since 25 May 2018 (status: 1st December 2019).***

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

With regard to complaint handling, it is standard approach with the CNPD to order the controller to comply with the data subject's requests to exercise his or her rights pursuant to the GDPR and/or to order the rectification or erasure of personal data should the situation require it.

c. Are you resolving any possible infringements of the Regulation with the help of so-called "amicable settlements"?
Although there is no specific provision in the Luxembourg data protection act referring to an "amicable settlement" per se, the CNPD always seeks to resolve the cases in a conciliating way between the controller and the data subject.
d. How many fines did you impose since May 2018? Please provide examples.
N/A
e. Which attenuating and or aggravating circumstances did you take into account?
N/A

Please find hereafter the requested national statistics on data breaches and - National initiatives to give guidance to SMEs or any other specific support to the SMEs.

With regard to statistics on data breaches, the CNPD has received 498 data breach notifications between 25 May 2018 and 1 December 2019.

With regard to LU SA initiatives towards controllers in general, including SME's (SMEs represent >90% of LU based companies and 55% of local employment):

- ***Providing general advise via e-mail and phone hotline for SMEs contacting CNPD for guidance;***
- ***Monthly newsletter to 1700 subscribers;***
- ***Simplified and structured form for Databreach notifications designed in a way to guide controllers in their analysis of the data breach;***
- ***Development of a GDPR maturity self-assessment tool (for businesses in general) which is an innovative, intuitive solution enabling users to check the level of coverage of their organizations against the GDPR requirements;***
- ***Organisation of workshops (open data protection laboratories "DaProLab") dedicated to DPOs and business managers from SMEs (and other organizations);***
- ***Joint trainings for business owners of SMEs with their professional business association on identifying their stakeholders in the context of GDPR;***
- ***Publication of a guidance for employers and employees on surveillance on the working place;***
- ***Participation in conferences and events addressed to young businesses and entrepreneurs (startups).***