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

ANSWERS FROM THE FRENCH 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)?

At the CNIL, we mostly receive questions concerning the Privacy Shield in the context of the hotline we have. However, we have received a few questions concerning the Swiss adequacy decision, and occasionally on the Canadian and Israeli ones.

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 scope of the Canadian Federal legislation was modified, the EDPB in this regard answered a request of position from the Council concerning WADA.

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

We consider that the priority should be to first assess and update the existing adequacy decisions instead of considering adopting new ones.

In any case, should there be any new draft adequacy decision to be adopted, the EDPB should this time be consulted sufficiently in advance to be able to perform its independent assessment and issue its opinion when consulted by the European Commission. In addition, the CNIL could like to recall that in this context, according to Article 70, s), "the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation." The CNIL underlines that this documentation shall in this context be made available in an easily understandable language (ideally French or English).

II. CHAPTER VII

The GDPR provided for one single set of data protection rules for the EU (by a Regulation) and one interlocutor for businesses and one interpretation of those rules. This "one law one interpretation" approach is embodied in the new cooperation mechanism and consistency mechanisms. In order to cooperate effectively and efficiently the GDPR equips the Data Protection Authorities (thereafter the DPA/DPAs) with certain powers and tools (like mutual assistance, join operations). Where a DPA intends to adopt a measure producing effects in more than Member State, the GDPR provides for consistency mechanism with the power to ask for opinions of the European Data Protection Board (EDPB) on the basis of Article 64(1) and (2) GDPR. In addition, in

situations where the endeavour to reach consensus in the cases of one-stop shop (OSS) does not work (i.e. there is a dispute between the DPAs in specific cases), the EDPB is empowered to solve the dispute through the adoption of binding decisions.

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

1. Cooperation Mechanism

1.1. OSS – Article 60

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

The CNIL is involved in many OSS cases.

Concerning Article 60 procedures, on November 27th, independently of data breach notifications, the CNIL had initiated 15 draft decisions, adopted 9 final decisions and sent 8 informal consultations to share information, opinion or submit a position to other DPAs. On November 27th, the CNIL was involved in many OSS cases handled by other DPAs. It has received and assessed 82 draft decisions (76 are final now) and 172 informal consultations.

For data breach notifications, we follow the guide “Draft Databreaches in IMI Version B 1.0”:

- We use the article 60 IC
    - As LSA in order to inform the other CSA that we have a case to share with them;
    - As CSA in to follow up with the LSA the action taken by the controller or the SA.

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

For now, we did not encounter proper obstacles. Cooperation mechanisms are all new tools that the authorities have had to embrace. They still have to find ways to make them as appropriate as possible and improve efficiency.

In addition to these new tools, the difference of methodologies, interpretation of the provisions of the Regulation, maturity and/or national procedural laws of DPAs can generate inconvenience and expectations on the part of the authorities concerned.

It appeared for instance that some DPAs consider they have always to assess the admissibility of a complaint regarding their own criteria, including when they act as LSA on the basis of complaints launched with another DPA. This could lead a LSA to refuse to handle a complaint, although deemed admissible by the complaint receiving DPA.

As CSA for data breach notifications, having the "Mandatory Form - minimum set of data- to be used when exchanging data between DPA" file discussed together with the Technology Subgroup is a good and important thing as we know with kind of information we've and where to find them.

We've never faced any problems or obstacles in the cooperation process, from the point of view of LSA or CSA. Regarding the DBN part, if an enforcement was necessary on a case, it would be transferred to the investigations department and not be handle anymore by the department in charge of DBN.

We've never faced the necessity to push or come back to a LSA in order to have information. On the DBN topic, we let the LSA working on the case, we've never faced the necessity to ask for more information (the description made inside the case and the "mandatory form" are, so far, enough in order to have a point of view on the breach and the action to come).

Having the "Draft Databreaches in IMI Version B 1.0" document is also really interesting and important for us (as well as the IMI user guide) as the software and the logic of managing information inside it is not really easy or user friendly (i.e. 3 clicks in order to add a country as supposed CSA when performing an article 56, when we've got a DBN with 15 countries involved, it's too many click).

More generally, even if cooperation is time consuming and it can be difficult to reach agreement, we appreciate the value of our exchanges with our counterparts and believe it is a prerequisite for the success of the GDPR.

We therefore devote a lot of resources and time to it.

c. How would you remedy these problems?

It seems to us that strengthening communication between authorities is the best way to ensure that they understand each other better and work better together. The IMI platform is a good way to communicate although the information system should be further adapted to the needs of SAs and improved to offer a more user-friendly and efficient tool to the SAs. The authorities also deploy other means of communication such as regular bilateral contacts, conference calls, etc. Some issues are also raised to the EDPB level (expert working group or even Plenary).

The mechanism of joint operations should also be explored. It seems to be a very good way to improve cooperation, to work on common positions but also on common methods.

All authorities must also be prepared to compromise. They must agree to review their positions, their internal practices and national procedures in order to achieve the coherence to which the GDPR tends.

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 administrative procedure is compatible with the OSS mechanism. The CNIL worked and adopted opinions on the draft law in order to ensure this compatibility. The CNIL also has reviewed its practises to make them compatible with the OSS mechanism.

It is clear that any decision of issuing a corrective measure has to be submitted to other CSAs.

However, the handling of a complaint usually does not lead to a corrective measure but to a resolution of the case through the intervention of the CNIL who acts as an intermediary between the complainant and the data controller. For example, with regard to the exercise of rights, the fact that the controller is complying with the request of the data subject will most often lead to the closure of the procedure. In that case, the CNIL previously did not issue any decision to close the case with the controller but only with regard to the complainant.

Since the GDPR entry into application, a cross-border complaint handled by the CNIL as LSA is always subject to a draft decision with regard to the controller to ensure the correct application of article 60.

Even in that case, where the request of the complainant had been satisfied, the CNIL submits a draft decision to close the complaint to concerned DPAs explaining that the controller has satisfied the complainant request and/or made significant changes to his practices through the intervention of the CNIL so that the CNIL decided to simply close the case.

The complainant is not considered as a party as such. Even if the complainant is related to the exercise of a right, the CNIL does not ask properly to the complainant whether or not he/she is satisfied with the measures taken by the controller. In fact, it is the role of the CNIL to determine what is sufficient or not to fulfil GDPR's obligations. When the complaint is related to more general obligations (information and transparency, retention period, security…) the CNIL considers that the complaint plays a warning role and that it is up to the CNIL to determine the standard of what is or is not compliant with the law.

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 some cases, we have already considered that we were in the situation where Article 56(2) could apply because the issue only affect the complainant which is a French date subject and there is an establishment of the data controller in France. We informed the LSAs which decided not to handle the case. However we faced the issue that controllers are not familiar with Article 56 (2) provision. One controller answered saying that it took measures to resolve the individual problem at stake but pointed that it will refuse to be in contact with the CNIL which is not the LSA since its main establishment is not in France.

Although the CNIL considers that this derogation is a very good way to handle simple complaints in a faster way, it is a bit early to draw conclusions about this mechanism.

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

The limited number of decisions submitted through IMI by DPAs makes it difficult to estimate if the OSS is at the level of expectations.

As to difficulties encountered, we would mention the differences of national legislation and administrative procedures between member states as the prominent issue so far. It makes the cooperation mechanisms even more difficult to set up and compromises the coherence to which the GDPR tends.

1.2. Mutual assistance – Article 61

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

We mainly use Article 61 to ask another DPA to handle complaints or to ask for information about a controller or a specific processing to another DPA.

For data breach notifications, Article 61 – voluntary mutual assistance should be used in order to share information about a DBN for which no LSA is identified. We've never used this possibility as we always have input on LSA and supposed CSA. The discussion on these points are conducted inside the Art. 56 procedure (identifying LSA and CSA).

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?

Since we have used it very little to properly request the provision of information, an update of the progress of a complaint or supervisory measures, it is hard to tell. However, it seems to us that this is an interesting tool to require another DPA to take concrete action.

d. Do you encounter any other problems preventing you from using this tool effectively? How could they be remedied?

We did not encounter any problem. As this tool is bilateral, it seems preferable to us to opt for a more informal contact at first, by sending an email for example, in order to maintain good and fluid relations with our European colleagues.

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?

Not yet.

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

No.

c. Is it effectively facilitating your work? If yes, how? If not, why?

n/a

d. Did you encounter any problems (e.g. of administrative nature) in the use of this tool? How could they be remedied?

n/a

2. Consistency mechanism

2.1 Opinion - Article 64 GDPR

a. Did you ever submit any draft decision to the Board under Art 64(1)?

We submitted 2 draft decisions concerning DPIA lists (the compulsory ones and the white list).

We also submitted a draft decision concerning the accreditation requirements for the monitoring bodies (article 41 GDPR).

Concerning certification, we have not yet submitted any draft, but Art 64(1) will only apply when a competent supervisory authority intends to adopt criteria for the national certification referred to in Article 42(5).

Lastly, we will probably submit a draft decision concerning BCRs in the first semester of 2020.

b. Did you ever submit any draft decision to the Board under Art 64(2)?

Yes the French, the Swedish and the Czech data protection authorities requested the Board to examine and issue an opinion on continuance of the competence of a national authority in case of a change in circumstances relating to the main or single establishment.

The submission of the request led to an opinion of the Board in July 2019.

This procedure will also be used for the approval of EU Data Protection Seal by EDPB according to Article 42(5).

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 deadline foreseen under the GDPR of 2 weeks is very short to comply as well with our procedural rules, but on the substance we did not encounter any issue so far.

d. Was the “communication of the draft decision” complete? Which documents were submitted as “additional information”?

No « additional information » were submitted.

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

For the documents exchanged, we had no issues as they were drafted in English. Nevertheless, the translation into French of the guidelines adopted took quite a long time.

f. Does that tool fulfil its function, namely to ensure a consistent interpretation of the GDPR?

2.2 Dispute resolution - Article 65 GDPR

a. Was this procedure used? If yes, what was your experience during the process?

Not 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?

Not yet.

3. Exchange of information: Standardised communication

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

A tool such as IMI is essential for cooperation and communication between authorities, in particular as regards multilateral contacts.

However, the operating procedures of this tool are binding. Inserting cases into IMI and following-up cases is time-consuming. This has considerably changed the tasks of some officers at the CNIL, in particular in our European and international department and in our complaints department.

A dedicated position will be created in January in the complaints department for a person to take charge of this demanding mission of introducing cases in IMI, monitoring and updating them.

In the context of Article 64 procedures, the absence of link between the number of the inital request for opinion and the number of the opinion issued by the EDPB complicates the follow-up of the procedure. It would be easier to have the same number of file all along the process.

Also, the notifications in IMI are not really convenient, as it would be more efficient to receive targeted notifications, in particular when a new document or a new comment is added rather than for each new action undertaken by a user.

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.

Année	2016	2017	2018	2019	2020
Postes budgétaires	198	199	200	215	225

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	2017	2018	2019	2020
Budget total	**18 853 380**	**17 035 799**	**17 395 563**	**18 506 734**	**20 143 889**
dont masse salariale	13 842 841	14 088 832	14 402 426	15 162 970	/
dont fonctionnement	5 010 539	2 946 967	2 993 137	3 343 764	/

c. Is your DPA dealing with tasks beyond those entrusted by the GDPR? If yes, please provide an indicative breakdown between those tasks and those entrusted by the GDPR.

Yes, the CNIL is also competent to apply for instance:

- the Directive Eprivacy (cookies and SPAM);
- the Directive (EU) 2016/6801;
- the French legislation applicable to activities which fall outside the scope of Union law (national security);
- the French legislation applicable to activities which fall outside the scope of the GDPR (personal data of deceased persons).
- PNR Directive implementing law
- Coordinated supervision of EU agencies and large scale systems together with the EDPS
- Government registers (all national registers)
- National law on credit data
- Scientific research specific laws
- Others (when there is a processing of data)

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

HR of the CNIL (225 positions in 2020) are not enough compared to the missions entrusted to the CNIL to answer the main issues at stake, which are:

[1] Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties

- Preventing a weakening of the enforcement chain, which dimension changed with the GDPR, and progressively reducing the gap between the control capacity of the CNIL, on the one hand, and the size and complexity of the ecosystem to control (all the controllers and processors established in France or targeting the French territory) on the other hand.
- Providing, in this transition period, legal certainty which the operators expect when consulting/seizing the CNIL (thousands of consultation requests, processing of more than 2 000 data breach notifications during the first year of the GDPR, answers to the 16 000 electronic requests of information received, editorial animation of a website which counts more than 8 million visits, etc), as well as the public authorities (more than 130 opinions issued on draft texts in 2018, as well as informal consultations led before or independently of a formal request).
- Avoiding that the stock of complaints skyrockets, which is inevitable with a steady number of staff (despite productivity gains constantly sought with determination and efficiency so far), and which will soon call for a vigorous reaction from the public authorities if nothing is done in 2020.

Financial resources are up to the needs in this context, however they imply an ongoing vigilance to be maintained.

Technical resources are taken into account in the context of a pluriannual IT master plan which allows the CNIL to answer the requirements it is facing.

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?

The CNIL lacks HR to effectively contribute to all cooperation mechanisms. Indeed, it keeps asking every year its competent public authorities to grant it more positions, stressing the needs in terms of cooperation tasks and the tight deadlines foreseen under the GDPR, which both command the CNIL to take action in certain situations.

Currently, around 70 persons use IMI more or less often at the CNIL, among whom around 30 persons use it often (most of them at least on a weekly basis). A dedicated position has also been created in the complaint department to work almost exclusively on IMI.

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?

The CNIL received 17 655 complaints between 25th May 2018 and 30th November 2019.

14 118 complaints were handled by CNIL's complaints Department.

The rest (3 537) was handled by the front-office Department of the CNIL in charge of the relations with the public, as these complaints were not considered as admissible (i.e the one month delay for the data controller to respond to a data subject request is not over at the time the complaint is lodged).

The CNIL qualifies as a complaint:

A request lodged by a data subject about the processing of personal data relating to him or her;

A request lodged by a not-for-profit body, organisation or association with the mandate of almost one data subject concerned;

A request made by a not-for-profit body, organisation or association about a processing of personal data, without any mandate of a data subject.

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

Warnings, reprimands, orders to bring processing operations into compliance and fines, order to comply with data subject's requests to exercise individual rights, order to communicate a data breach to the data subject, additional powers under national law (order under a daily penalty)

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

The notion of "amicable settlement" is not envisaged in the French data protection legal system.

However, the handling of a complaint usually leads to a resolution of the case through the intervention of the CNIL, who acts as an intermediary between the complainant and the data controller.

With regard to the exercise of rights, the fact that the controller is complying with it will most often lead to the closure of the procedure. So in a way, it has similar effects as an amicable settlement.

On the other hand, with regard to more general obligations (information and transparency, retention period, security…), breaches of the law are more "public policy" and therefore the CNIL would not ask the complainant whether or not he agrees with the measures taken by the controller. We consider that the complaint plays a warning role and that it is up to the CNIL to determine the standard of what is or is not compliant with the law.

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

The restricted committee of the CNIL has imposed 15 fines since May 2018.

For instance: 50 million euros on GOOGLE; 400 000 euros on SERGIC; 180 000 on ACTIVE ASSURANCES; 500 000 on FUTURA INTERNATIONALE.

You can find more information about the sanctions pronounced by the CNIL on its website: https://www.cnil.fr/fr/les-sanctions-prononcees-par-la-cnil.

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

Some aggravating circumstances that have been taken into account are, among others: the number of data subjects concerned, the lack of cooperation with the CNIL, the categories of data concerned or the duration of the violation.

Additional questions:

- National statistics on data breaches

With regards to the number of data breach notifications, the CNIL received 3 273 notifications between 25 May 2018 and 31 December 2019. These figures correspond to the numbers of files/cases, this means that for some of them we might have received an initial notification and additional ones later on.

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

Concerning national initiatives to give guidance to SMEs or any other specific support to the SMEs, we have developed/provided the following tools in France:

- a dedicated pack available on the website of the CNIL, with a practical guide and forms (https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement);

- a video with a Youtuber on how to apply the GDPR (https://www.cnil.fr/fr/video-le-youtubeur-cookie-connecte-repond-vos-questions-sur-larrivee-du-rgpd);

- a simplified register (available in French: https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement as well as in English https://www.cnil.fr/en/record-processing-activities);

- a MOOC (https://www.cnil.fr/fr/la-cnil-lance-sa-formation-en-ligne-sur-le-rgpd-ouverte-tous);

- specific content concerning security and a guide (https://www.cnil.fr/fr/securite-des-donnees).

We have also several tools which are not specifically dedicated to SMEs but which are used by them a lot:

- a hotline;

- FAQs on the website;

- the DPIA software;

- the white list for processing exempted from DPIA;

- a notification form available online (developed within the EDPB).