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

ANSWERS FROM THE ITALIAN SUPERVISORY AUTHORITY

The General Data Protection Regulation ('GDPR') entered into application on 25 May 2018, repealing and replacing Directive 95/46/EC. The GDPR aims to create a strong and more coherent data protection framework in the EU, backed by strong enforcement. The GDPR has a two-fold objective. The first one is to protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. The second one is to allow the free flow of personal data and the development of the digital economy across the internal market.

According to Article 97 of the GDPR, the Commission shall submit a first report on the evaluation and review of the Regulation to the European Parliament and the Council. That report is due by 25 May 2020, followed by reports every four years thereafter.

In this context, the Commission shall examine, in particular, the application and functioning of:

- Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC; and
- Chapter VII on cooperation and consistency.

The GDPR requires that Commission takes into account the positions and findings of the European Parliament and the Council, and of other relevant bodies and sources. The Commission may also request information from Member States and supervisory authorities. As questions related to Chapter VII concern more directly the activities of the DPAs, the present document focuses primarily on that aspect of the evaluation, while also seeking their feedback on Chapter V related issues.

We would be grateful to get the replies to the questions (in English) by 15 January 2019, at the following e-mail address: JUST-EDPB@ec.europa.eu.

Please note that your replies might be made public.

When there are several DPAs in a given Member State, please provide a consolidated reply at national level. In the context of the preparation of the evaluation report, and following the input from other stakeholders, it is not excluded that we might have additional questions at a later stage.

I. CHAPTER V

The GDPR provides that the adequacy decisions adopted by the Commission under Directive 95/46 remain in force under the GDPR until amended, replaced or repealed. In that context, the Commission is tasked to continuously monitor and regularly evaluate the level of protection guaranteed by such decisions. The 2020 evaluation provides a first opportunity to evaluate the 11 adequacy decisions adopted under the 1995 Directive. This does not include the decision on the Privacy Shield that is subject to an ad hoc annual review process and the Japanese adequacy decision that was adopted last year under the GDPR and is also subject to a specific evaluation exercise (the first one will be in 2021).

1. Has any stakeholder raised with your authority any particular question or concern regarding any of the adequacy decisions adopted under the 1995 Directive (with the exception of the EU-US adequacy decision which is not covered by this evaluation process)?
   No, we have not received specific questions regarding any of the adequacy decisions adopted under the directive 95/46.
2. Does your authority have any information on the developments of the data protection system of any of the countries/territories subject to a Commission adequacy decision under the 1995 Directive that you would consider relevant for the Commission's evaluation?
   No.

3. In your view, should any third country or international organisation be considered by the Commission in view of a possible adequacy decision?
   We would suggest considering the international organisations, especially those working in the field of humanitarian law and human rights; additionally, those countries mentioned in the COMM communication of June 2019 (2019/374) are suitable candidates as well as Albania and San Marino.

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?
   Yes. We would suggest referring to the statistics of the IMI systems to reply to this question in a coordinated manner.

b. Did you encounter any problems/obstacles in your cooperation with the lead/concerned DPA? If yes, please describe them
   We believe some of those problems to consist in the following:

- Differences in national administrative law procedures, in particular as regards the handling of complaints and the criteria for considering such handling completed along with the handling of requests for access to documents/comments circulated under the IMI system;
- Different notions of 'draft decision' pursuant to Article 60 (3);
- Different approach relating to the applications of fines, again resulting mainly from different national procedural rules.

We have not yet encountered but envisaged difficulties in applying penal sanctions set out only in a national law which is not the one of the LSA. We wonder in particular how to reconcile the OSS with the requirements under national law whereby the 'local' SA must report the criminal infringements to the competent national judicial authority and how to prevent 'ne bis in idem' situations (especially in case very high fines are to be imposed on the controller by the LSA) – see Recital 149 GDPR.

c. How would you remedy these problems?
The work in progress in several ESGs, has helped and is helping cope with several implementing difficulties in order to find a streamlined, harmonised approach.

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?)
Yes, see in particular the rules of procedures set out in the Italian SA's internal Regulation 1/2019.

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)?
Yes, in some cases. We would suggest referring to the statistics of the IMI systems to reply to this question in a coordinated manner.

f. Is the OSS living up to its expectations? If not, what would you identify as its shortcomings? How can they be remedied?
Perhaps it is a bit too early to reply meaningfully to this question. Generally speaking, the timeframe envisaged by the GDPR creates difficulties that the authorities are trying to reduce by means of an informal cooperation phase. Moreover, too many 'minor' cases (especially relating to non-compliance with individual exercise of rights requests) are seemingly uploaded to IMI, which in fact may be resolved, inter alia, by a larger use of amicable settlements.

1.2. Mutual assistance – Article 61

a. Did you ever use this tool in the case of carrying out an investigation?
Yes but the procedures are still pending.

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, considering that it helps exchanging information among the authorities; however, the fact that a 'special' voluntary mutual assistance procedure has been introduced operationally shows that there is room for improvement also in this area. Once again, we are afraid that it is too early to provide a full-fledged evaluation considering the limited experience in applying it.

d. Do you encounter any other problems preventing you from using this tool effectively? How could they be remedied?
There is a certain hesitation in using this tool because of the possible consequences in case of non-compliance with an assistance request (risk of an Article 66 procedure, etc.).

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, but we are envisaging to use it in several cases.

b. Did you ever use this tool in the case of monitoring the implementation/enforcement of a measure imposed in another Member State?
Not yet.

c. Is it effectively facilitating your work? If yes, how? If not, why?
Too early to reply to this question.

d. Did you encounter any problems (e.g. of administrative nature) in the use of this tool? How could they be remedied?
Not yet.

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, we submitted a draft decision under Article 64.1.a.

b. Did you ever submit any draft decision to the Board under Art 64(2)?
No. However, we submitted a request for an opinion under Art 64(2) which was withdrawn because it was ultimately found not to be in line with the applicable criteria.

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.
There was no clear procedure to ensure that the changes made to the draft decision were fully in line with those requested by the Board. Even if some amendments to the RoP of the Board have been made, clearer wording in the GDPR would help clarify this point.

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

Yes; no additional information was necessary for the case at issue.

e. Were there any issues concerning the translations and/or any other relevant information?
No.

f. Does that tool fulfil its function, namely to ensure a consistent interpretation of the GDPR?
It appears it does help ensure consistency even though there are some implementing issues, e.g. as for the approval of the European Data Protection Seals (i.e. no approval decision of the Board is envisaged by the GDPR even if Art. 57 envisages that it should be adopted by the Board) and as for the approval of BCRs (according to a literal interpretation of Art. 64.1 and 64.7, each CSA would have had to present a draft decision to the Board for the approval of the same BCRs – the issue has been resolved by envisaging a specific cooperation procedure for the approval of the BCRs only by the LSA). The same issue could be raised for other instruments in Article 64.1 (e.g. code of conducts).
As for the transfer instruments envisaged in Article 46.3, even if Article 46.4 envisages the application of the consistency mechanism, only Art. 46.3.a is listed among the cases in which an opinion of the Board under Art. 64.1 should be requested by the LSA. In order to solve this inconsistency, an opinion under Art. 64.2 has been requested to deal with cases relating to Art. 46.3.b.
An overarching consideration in this respect has to do with a certain rigidity of the Article 64 procedure both as for the timing and as for some loopholes that the Board has been tackling by creating informal cooperation procedures (see above).

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?
//

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?
No.

3. Exchange of information: Standardised communication

a. What is your experience with the standardised communication through the IMI system?
It is helpful although it has the usual criticalities of any standardised approach – i.e., it does not allow introducing ad-hoc specifications.

4. European Data Protection Board

a. Can you provide an indicative breakdown of the EDPB work according to the tasks listed in Article 70?
In terms of workload, the EDPB has been working mostly on Articles:

- 70.1.a (monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities);
- 70.1.e (examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation);
- 70.1.s (provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection.);
- 70.1.t (issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64.1, on matters submitted pursuant to Article 64.2).

In general, the EBPB's activity has been focused on consistency rather than cooperation procedures.

b. *For the EDPB Secretariat*: Can you provide an indicative breakdown of the EDPB Secretariat work and allocation of resources (full-time equivalent) according to the tasks listed in Article 75?

5. Human, technical and financial resources for effective cooperation and participation to the consistency mechanism

a. How many staff (full-time equivalent) has your DPA? Please provide the figures at least for 2016, 2017, 2018, 2019 and the forecast for 2020.
2016: 113 permanent staff + 8 contract staff; 2017: 116 permanent staff + 8 contact staff; 2018: 170 positions; 2019: 170 positions; forecast for 2020: 170 positions.

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: 19.889.832 (source Annual Report 2016); 2017: 21.061.841,95 (source: Annual Report 2017); 2018: 26.927.498 (source Annual Report 2018); forecast for 2019: 29.127.273; forecast for 2020: € 30.127.273,00.

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 Italian SA is competent for dealing with complaints under Law No 71/2017 containing provisions to protect minors for the prevention and fight against cyberbullying, and for dealing with complaints related to exercise of the rights set out in Articles 15 to 22 in respect of deceased persons.
The Italian SA is also the competent supervisory authority for the supervision of the application of the Directive 2002/58/EC, and accordingly (with regard to Article 13 of the latter) of Regulation 2006/2004 on cooperation for consumer protection (now replaced by Regulation 2017/2394); furthermore, it is the competent supervisory authority for processing activities under directive 2016/680 (law enforcement directive) pursuant to the national transposition legislation (Decree No 51/2018), under directive 2016/681 (EU PNR Directive), under Regulation 2019/493 to prevent inappropriate use of personal data in the context of EP elections, and for supervising national

security activities (in accordance with specific procedures set out in Section 58 of legislative decree No 196/2003).

The Italian SA discharges supervisory or assistance tasks concerning personal data processing as provided for by laws ratifying international agreements and conventions or else by Community or EU regulations (such as the ones on: the second-generation Schengen Information System (SIS II); European Union Agency for Law Enforcement Cooperation (Europol); 'Eurodac'; VIS Regulation; 'the IMI Regulation'; Chapter IV of Convention No. 108).

Furthermore, in line with Article 58.6 GDPR, the following additional powers have been conferred on the Italian SA by the national law adjusting the domestic legal system to the GDPR. More specifically, the Italian SA is empowered to:

"a) verify whether data processing operations are carried out in compliance with applicable laws and regulations, also in case of termination of processing and with regard to the storage of traffic data[1];

b) handle the complaints lodged with it in pursuance of the Regulation and the provisions of this Code, by also laying down specific arrangements in that respect through its rules of procedure and setting the priority issues as resulting annually from such complaints, which issues may then become the subject of investigations in the course of the relevant year;

c) encourage the adoption of rules of conduct in the cases mentioned under Section 2-c;

d) report facts and/or circumstances amounting to offences to be prosecuted ex officio, which it has come to know either in carrying out or on account of its functions;

e) transmit the annual report as drawn up pursuant to Article 59 of the Regulation to Parliament and Government by the 31st of May of the year following that to which the report refers;

f) ensure the protection of the fundamental rights and freedoms of the individuals by implementing the Regulation and this Code as appropriate;

g) discharge such tasks as are allocated to it by Union or State law and carry out such additional functions as are laid down in domestic law.".

With regard to the above additional powers, the Garante is tasked in particular with:

a. Carrying out annual security audits on the national population register, under the terms of Section 62 of legislative decree No 82/2005;
b. Issuing an opinion on any review request submitted to the anti-corruption and transparency officers (or to the competent Ombudsperson, where regions or local authorities are concerned) whenever FOIA-type access requests are rejected, remain unanswered or are deferred on personal data protection grounds; the Garante's opinion must be acquired on a mandatory basis pursuant to Section 5(7) and (8) and Section 5-a of legislative decree No 33/2013;
c. Supervising operation of 'SPID', i.e., the public system for management of the digital identity of citizens and businesses, under Section 30-a of the SPID implementing regulations;
d. Carrying out checks on the public opt-out register to counter unsolicited direct marketing (Section 12 of Presidential decree No 178/2010);
e. Supervising operation of the national DNA database at the Minister of the Interior – Public Security Department (Presidential decree No 87/2016);

[1] As amended by section 4(1) of legislative decree no. 109/2008 (implementing directive 2006/24/EC).

f. Issuing opinions on requests for access to administrative records containing personal data, upon request of the competent Committee for the access to administrative records (Law No 241/1990);
g. Supervising the services committed to call-centres located outside the EU, and imposing the relevant sanctions, pursuant to Law No 232 of 11 December 2016.

d. How would you assess the resources from your DPA from a human, financial and technical point of view?
We would need to increase our staff (also IT staff) and our budget in order to perform all tasks entrusted to our Authority and ensure effective implementation and enforcement of the GDPR.

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?
We are not yet fully equipped to contribute to the mechanisms. We have staff (around 10 people) working on cross-border cases along with the national cases within our Departments.

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 up to 30 November 2019, we received 13,877 complaints (in particular we received 2,914 'complaints' *strictu sensu* according to Article 142 of the Italian Data Protection Code, i.e. a complaint specifying, in as detailed a manner as possible, "the underlying facts and circumstances, the allegedly infringed provisions and the remedies sought and [containing] the identification data concerning the controller and the processor, if known", and 10,963 alerts).

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

The Garante used the following corrective powers:
1) warnings under art. 58.1.a GDPR;
2) reprimands (art. 58.2.b GDPR);
3) orders to the controller or the processor to comply with the data subject's requests to exercise his or her rights (art. 58.2.c GDPR);
4) orders to the controller or processor to bring processing operations into compliance with the provisions of this Regulation (art. 58.2.d);
5) orders to the controller to communicate a personal data breach to the data subject (art. 58.2.e GDPR);
6) a temporary or definitive limitation including a ban on processing (art. 58.2.f GDPR);
7) administrative fines (art. 58.2.i GDPR).

c. Are you resolving any possible infringements of the Regulation with the help of so-called "amicable settlements"?
Yes. Regarding complaints related to exercise of the rights set out in Articles 15 to 22 of the GDPR, amicable settlement attempts are carried out by the SA within 45 days of receiving the complaint

(still after vetting the complaint for admissibility); the SA serves the admissible complaint on the controller and jointly invites the latter to comply with the data subject's request within 20 days and to inform the complainant thereof. If the controller complies in full, the SA informs the complainant thereof under Article 77(2) GDPR and notifies the controller of the possible initiation of a proceeding to decide on the application of corrective measures (if any), including fines.

For complaints unrelated to exercise of the rights set out in Articles 15 to 22 of the GDPR, an amicable settlement attempt may be made by the SA in the preliminary investigation phase (after vetting the complaint for admissibility); in that case, the deadline for the controller to comply with the measures sought by the complainant is set by the SA. The SA will then decide on the subsequent steps, if any, also with a view to the application of corrective measures (under Section 14 of the internal Regulation). The complainant is informed in any case of the progress or outcome of this procedure pursuant to Article 77(2) GDPR.

In any case, the achievement of an amicable settlement is taken into consideration when determining the corrective measure to be taken and, if imposition of a fine is envisaged, it is considered as an attenuating circumstance under Article 83.2.f.

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

The Garante has been working throughout 2018 and 2019 mainly to deal with the substantial backlog of fining procedures relating to pre-GDPR infringements. Accordingly, 366 fining procedures were started prior to 25 May 2018 and led to 80 fining injunctions issued afterwards, whilst 86 fining procedures were started after 25 May 2018 and led in 19 cases to payment of a reduced fine as provided for in pre-GDPR procedural rules – as said, all the above fining procedures had to do with pre-GDPR infringements. In additional 800 pre-GDPR cases where fining procedures had been started prior to 25 May 2018, the amounts of the leviable fines as notified to the controllers involved have become due afterwards on account of specific provisions in the decree adjusting the national legal system to the GDPR (Section 18 of Decree No 101/2018).

As for post-25 May 2018 infringements, the Garante imposed three fines; two of them were imposed on public bodies.

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

The Garante took into account the following attenuating or aggravating circumstances:

1) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them (Article 83.2.a);
2) any action taken by the controller or processor to mitigate the damage suffered by data subjects (Article 83.2c);
3) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32 (Article 83.2.d);
4) any relevant previous infringements by the controller or processor (Article 83.2.e);
5) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement (Article 83.2.f);
6) the categories of personal data affected by the infringement (Article 83.2.g);
7) the provisions set out in Section 22(13) of legislative decree 101/18 regarding the imposition of sanctions in the initial eight months of implementation of the new regulatory framework.

- National statistics on data breaches

  Since 25 May 2018 up to 30 November, the Garante received 1,951 data breach notifications.

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

  We are involved in the SMEDATA project, co-funded 80% by the European Commission, which aims to ensure the effective application of the General Regulation on the Protection of Personal Data through awareness-raising, the multiplication of training and the sustainable development of capacities for SMEs and legal professions. As part of this project, we carried out the following activities:

  • we have organized, in partnership with Roma Tre University, 12 regional awareness-raising events for SMEs and legal professionals (2 in Milan, 2 in Genoa, 2 in Florence, 2 in Rome, 2 in Salerno and 2 in Cosenza). We will organize two events for trainers in Rome by April 2020;

  • we have organized two events attended by more than 60 representatives of trade associations and associated companies, and universities, in order to adopt a self-assessment tool for sustainable awareness based on SMEs' specific needs and processes from the perspective of personal data protection;

  • we have developed, with the partners of the consortium, a mobile application as a free open-source software tool assisting citizens and SMEs in understanding and complying with GDPR;

  • to ensure that the results of this project are exploited to the maximum and disseminated on a large scale across Europe and among interested stakeholders, we will organize a dissemination campaign and communication of project results through the organization of an international conference to be held in Rome at the end of 2020.