



Report on the application of the GDPR under Article 97

Questions to Data Protection Authorities / the European Data Protection Board

Fields marked with * are mandatory.

1 Introduction

According to Article 97 of the GDPR, the Commission should submit a first report on the evaluation and review of the Regulation to the European Parliament and the Council by 25 May 2020, followed by reports every four years thereafter. The Commission's first report was adopted on 24 June 2020 (the '2020 report'). [1] The next report is due by mid 2024 (the '2024 report').

In this context, the Commission should 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 the 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.

Against this background, this document seeks to obtain the views of the European Data Protection Board on the abovementioned points. As was also done for the 2020 report, this document also seeks to obtain information from data protection authorities (DPAs) on their enforcement of the GDPR and on activities undertaken to promote awareness of data protection rights and obligations.

We would be grateful to receive replies to the below questions (in English) by **15 December 2023**.

In 2020, the European Data Protection Board provided a consolidated contribution of the individual replies of the DPAs to the questionnaire circulated in preparation of the 2020 report.[2] The Commission would be grateful if the Board would again provide such a contribution, in addition to providing the individual replies of DPAs. 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 report, and following the input from other stakeholders, it is not excluded that we might have additional questions at a later stage.

Please note that your replies might be made public or may be disclosed in response to access to documents requests in accordance with Regulation (EC) No 1049/2001.

[1] Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, 24.6.2020 COM(2020) 264 final.

[2] https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf

2 Supervisory Authority

* 2.1 Select your supervisory Authority

- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Denmark
- EDPS
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Iceland
- Ireland
- Italy
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Norway
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain

3 Chapter V

*** 3.1 In your view, should the data protection framework of any third country or international organisation be considered by the Commission in view of a possible adequacy decision?**

- Yes
 No

*** 3.2 If yes, of which third country or international organisation ?**

The countries to be prioritized will depend on the existence of cooperation mechanisms (article 50(1) GDPR) and of mutual assistance tools (article 50(2) of the GDPR which differ from one EEA member state to another.

As stated in the EDPB 2021 report on GDPR enforcement Luxembourg has not set up article 50 assistance tools with third countries.

With regards to personal data transferred to third countries in the context of international humanitarian action, the Commission may consider to focus on countries that have cooperation mechanisms in place with EU member states (for example with Luxembourg : Laos, Nicaragua, Burkina Faso, Cabo Verde, Mali, Niger and Senegal) Source: page 15, stratégie générale de la coopération luxembourgeoise.

*** 3.3 The Commission is interested in the views of the Board on the third countries for which enforcement cooperation agreements under Article 50 GDPR should be prioritised, in particular in light of the volume of data transfers, role and powers of the third country's supervisory authority and the need for enforcement cooperation to address cases of common interest. Please mention the countries that, in your view, should be prioritised and the reasons.**

See answer above.

3.4 Reasons for prioritisation if there should be any:

The volume of transfers, the sensitivity of the data transfers (e.g. in case of children data, medical data or humanitarian data) and the lack of a sufficiently robust data protection framework providing standards that assimilate to the GDPR.

3.5 Are there any other suggestions or points you would like to raise as regards tools for international transfers and/or enforcement cooperation with foreign partners?

Given the limited possibility of carrying out enforcement action via an article 27 representative and the lack of its liability (Section 2.6.4 of the EDPB report) statistics from EU member states could be gathered as to the countries that often appoint representatives and the possibility of pursuing MoU and further cooperation agreements with these countries.

4 Chapter VII

In July 2023, the Commission adopted a proposal for a regulation laying down additional procedural rules relating to the enforcement of the GDPR.[1] The DPAs and the EDPB provided extensive input to the Commission during the preparation of the proposal and following adoption, the EDPB and the EDPS adopted a joint opinion on the proposal on 19 September 2023.[2] The questions below focus on DPAs' application and enforcement of the GDPR and do not seek DPAs' views on the proposal.

[1] Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, COM/2023/348 final.

[2] https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-012023-proposal_en

4.1 Cooperation Mechanism

4.1.1 One-stop-shop (OSS) – Article 60 GDPR

The EDPB Secretariat will extract from IMI the numbers regarding the OSS cases where your DPA has been in the lead and concerned since 25 May 2018

The EDPB Secretariat will extract from IMI the numbers regarding whether your DPA has been 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).

4.1.1.1 Do you have any comment to make with respect to the identification and handling of local cases under Article 56(2) GDPR?

- Yes
- No

*** 4.1.1.3 Did you raise relevant and reasoned objections?**

- Yes
- No

4.1.2 Mutual assistance – Article 61 GDPR

*** 4.1.2.1 Did you ever use Mutual Assistance - Article 61 procedure in the case of carrying out an investigation?**

- Yes
- No

*** 4.1.2.3 Did you ever use Mutual Assistance - Article 61 procedure in the case of monitoring the implementation of a measure imposed in another Member State?**

- Yes
- No

*** 4.1.2.4 Could you explain why you have never used Mutual Assistance - Article 61 procedure for monitoring the implementation of a measure imposed in another Member State?**

There was no case where that procedure was deemed to be essential.

*** 4.1.2.5 What is your experience when using Mutual Assistance - Article 61 procedure?**

It always depends on the case. The procedure is mostly used to exchange information on a specific case.

4.1.3 Joint operations – Article 62 GDPR

* 4.1.3.1 Did you ever use the Joint Operations - Article 62 procedure (both receiving staff from another DPA or sending staff to another DPA) in the case of carrying out an investigation?

- Yes
 No

* 4.1.3.2 Could you explain why you have never used Joint Operations - Article 62 procedure for carrying out an investigation?

There was no case where that procedure was deemed to be necessary.

* 4.1.3.3 Did you ever use Joint Operations in the case of monitoring the implementation/enforcement of a measure imposed in another Member State?

- Yes
 No

* 4.1.3.4 Could you explain why you have never used Joint Operations - Article 62 procedure for implementation/enforcement of a measure imposed in another Member State?

There was no case where that procedure was deemed to be necessary.

4.2 Consistency mechanism

4.2.1 Urgency Procedure – Article 66 GDPR

* 4.2.1.1 Did you ever adopt any measure under the urgency procedure?

- Yes
 No

4.3 European Data Protection Board

The EDPB Secretariat will provide an indicative breakdown of the EDPB work according to the tasks listed in Article 70 GDPR and of the EDPB Secretariat resources allocated to complete the tasks listed in Article 75 GDPR, including on Article 64, 65 and 66 GDPR procedures, as well as on litigations.

4.3.1 How much resources (Full-time equivalent*day) does your DPA allocate to participation in EDPB activities?

	FTE*day
2020	5
2021	5,5
2022	6
2023	6,5
2024 (Forecast)	9

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

4.4.1 How many staff (full-time equivalent) has your DPA?

	FTE	Comments
2020	53	/
2021	54	/
2022	54	/
2023	60	/
2024 (Forecast)	66	/

4.4.2 What is the budget of your DPA? Please provide the figures (in euro)

	BUDGET (€)
2020	7 667 224
2021	7 200 000
2022	7 909 314
2023	9 262 771
2024 (Forecast)	10 278 653

* 4.4.3 Is your DPA dealing with tasks beyond those entrusted by the GDPR, including under the new EU legislation adopted under the Data Strategy?

- Yes
 No

* 4.4.4 Please provide an indicative breakdown between those tasks and those entrusted by the GDPR.

Apart from the tasks entrusted by the GDPR, the CNPD is responsible for monitoring and verifying that data subject to processing activities are processed in compliance with the provisions of the Act of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters (transposition of Directive 2016/680) and legal texts containing specific provisions relating to personal data protection (for example: law of 1 august 2018 concerning the processing of passenger name records, the Law of 30 Mai 2005 concerning the protection of private life in the electronic communications sector).

As to potential new missions based on the DGA, DSA, DMA, DA, the CNPD must wait what the future draft bills will foresee.

4.4.5 Please explain, if needed:

An indicative breakdown is not possible at the moment, as the CNPD does currently not know if the future government will foresee in the draft bills implementing the DGA, DSA, DMA, DA new missions for the CNPD.

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

	Sufficient	Insufficient
* Human Resources	<input checked="" type="radio"/>	<input type="radio"/>
* Financial resources	<input checked="" type="radio"/>	<input type="radio"/>
* Technical Means	<input checked="" type="radio"/>	<input type="radio"/>

* 4.4.7 is your DPA properly equipped to contribute to the cooperation and consistency mechanisms?

- Yes
 No

* 4.4.8 How many persons (FTE) work on the issues devoted to the cooperation and consistency mechanisms?

5

5 Enforcement

5.1 Complaints

5.1.1 The number of complaints (excluding requests for information) received by your DPA.

	2018	2019	2020	2021	2022	2023
Number of Complaints	71 IMI & 376 National = 447	227 IMI & 381 national= 608	155 IMI & 324 national = 479	147 IMI & 360 national = 507	126 IMI & 355 national = 481	69 IMI & 418 national = 487

5.1.2 The number of complaints where your DPA was in the lead

	2018	2019	2020	2021	2022	2023
The number of complaints received directly from complainants	376	381	324	360	355	418
The number of complaints received from another DPA through the OSS.	71	227	155	147	126	69

5.1.3 The number of complaints received by your DPA and forwarded to the lead DPA.

	2018	2019	2020	2021	2022	2023
Number of Complaints	9	16	9	13	7	2

5.1.4 The number of complaints relating to national cases resolved through a decision adopted by your DPA.

	2018	2019	2020	2021	2022	2023
Number of Complaints	5	5	5	5	5	5

5.1.5 The number of complaints relating to cross-border cases, resolved through an Article 60 GDPR decision adopted by your DPA[1]. Please indicate a breakdown of the decisions adopted under Article 60(7), (8) or (9) GDPR.

[1] This does not include amicable settlements.

	2018	2019	2020	2021	2022	2023
Number of complaints resolved through an Article 60(7) GDPR decision	0	0	0	0	17	34
Number of complaints resolved through an Article 60(8) GDPR decision	0	0	0	0	0	7
Number of complaints resolved through an Article 60(9) GDPR decision	0	0	0	0	0	0

5.1.6 The total number of complaints resolved through amicable settlement

	2018	2019	2020	2021	2022	2023
Number of Complaints	403	426	341	364	357	413

*** 5.1.7 What kind of communication or request do you qualify as a complaint?**

A complaint to the CNPD may be lodged electronically or by post mail.
In order to facilitate the filing of a complaint and in accordance with article 9 of the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework, the CNPD provides a complaint form which is available online on the website of the National Commission.
The CNPD benefits of the opportunity for action. It thus assesses on a discretionary basis whether or not a complaint shall be investigated. Depending on the characteristics of each complaint, the CNPD may decide not to investigate a complaint, taking into account, inter alia, the degree of severity of the alleged facts or the alleged violation, the degree of impact on fundamental rights and freedoms, the degree of priority in relation to the overall number of complaints and resources available.

5.1.8 For complaints handled by your DPA which you consider to be closed, provide the average and the median time (in months) from receipt of the complaint (either directly from the complainant or from another DPA) to closure (e.g. by decision or amicable settlement).

	In months
Average Time	9 months
Median Time	9 months

5.2 Own-initiative investigations

5.2.1 The number of “own-initiative” investigations launched by your DPA since 25 May 2018

	2018	2019	2020	2021	2022	2023
Number of Complaints	36	42	10	1	13	6

5.2.2 The number of these investigations that you consider to be closed. Provide the average and the median time (in months) from launch of the investigation to closure.

	2018	2019	2020	2021	2022	2023
Average Time	18-24 months	18-24 months	18-24 months	18-24 months	18-24 months	18-24 months
Median Time	14 months	14 months	14 months	14 months	14 months	14 months
Total number of closed investigations	34	41	10	1	8	0

5.3 Corrective measures

5.3.1 The number of decisions in which you used your corrective powers [1]

[1] Please reply per number of decisions, not per number of corrective powers used per decision. For instance, if one decision ordered both a ban and a fine, please reply "1".

	2018	2019	2020	2021	2022	2023
Number of Decisions	0	0	0	37	22	9

5.3.2 The number of times you used any other corrective power than fines. Please specify the type of measure by reference to Article 58(2) GDPR

	2018	2019	2020	2021	2022	2023
Issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation	0	0	0	0	0	0
Issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation	0	0	0	7	1	7
Order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation	0	0	0	0	0	0
Order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period	0	0	0	41	26	3
Order the controller to communicate a personal data breach to the data subject	0	0	0	0	0	0
Impose a temporary or definitive limitation including a ban on processing	0	0	0	1	0	1

Order 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	0	0	0	1	0	0
Withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met	0	0	0	0	0	0
Order the suspension of data flows to a recipient in a third country or to an international organisation.	0	0	0	0	0	0

5.3.3 The number of fines you imposed

	2018	2019	2020	2021	2022	2023
Number of Fines	0	0	0	25	20	3

5.3.4 Please provide examples of the type of circumstances and infringements that normally resulted in a fine and include the provisions of the GDPR breached.

The data controller did not ensure that the data protection officer (DPO) was involved in all issues which relate to the protection of personal data in accordance with article 38.1 of the GDPR. As he did not provide the DPO with the resources necessary to carry out his tasks in accordance with article 38.2 of the GDPR, the DPO could not carry out his duty to inform and advise the controller about his obligations in accordance with article 39.1.a) of the GDPR.

The data controller did not inform the data subjects in accordance with article 13 GDPR concerning the personal data collected via the video surveillance system, as well as via the Geo-tracking system. In addition, the ranges of several cameras were considered as disproportionate and in violation with article 5.1. c) of the GDPR and the appropriate technical and organisational measures to ensure a level of security appropriate to the risk were not implemented (article 32.1 GDPR).

The controller did not document internally two personal data breaches, he did not notify them to the CNPD and did not communicate them to the data subject as foreseen by articles 33.1, 33.5 and 34.1 of the GDPR. In addition, the appropriate technical and organisational measures to ensure a level of security appropriate to the risk were not implemented (articles 5.1.f) and 32.1. a) and b) of the GDPR) and on 25 May 2018, the data controller had not communicated yet the contact details of the data protection officer to the CNPD as required by article 37.7 of the GDPR.

5.3.5 The average and median level of fines and the total amount of fines imposed by your DPA

	2018	2019	2020	2021	2022	2023
Total amount of fines (€)	/	/	/	746319500	48375	6500
Average level of fine	/	/	/	29852780	2419	2167
Median level of fine	/	/	/	6700	1500	2500

5.4 Challenges to decisions in national courts

5.4.1 How many of your decisions finding an infringement of the GDPR have been challenged in national courts? Please provide the absolute figure and the percentage.

	Absolute figure	%
Decisions finding an infringement of GDPR challenged in national court	3	4,4
Successful challenges	No final decision yet	/

* 5.4.2 Where challenges were successful, what were the reasons of the national courts?

No final decision yet, all appeals are still pending before the administrative tribunal.

6 Promoting awareness of rights and obligations

* 6.1 Provide details of activities undertaken (publication of guidance, publicity campaigns, etc.) to promote awareness of data protection rights and obligations among the public and data controllers and processors. Where relevant, provide links to materials.

Since 2020, the CNPD has continued its efforts to raise awareness, in particular by taking part in conferences and workshops, by contributing to the development of training courses, by publishing information material such as the guidelines or by developing compliance tools.

Conferences, workshops and training courses

- The CNPD organized or participated actively in more than 50 conferences, training sessions and workshops:
 - o At the occasion of the International Data Protection Day, the CNPD organised over the last three years the following conferences « Cookies : Je tiens à ma vie privée ou je n'ai rien à cacher ? » , « Protection des données et de la vie privée face à la numérisation du travail » and « Le métavers : quelle réalité pour les droits et libertés de la vie privée ? » .
 - o Every year, the CNPD is giving training courses to the INAP (National Institute of Public Administration), the CSSF (Commission de Surveillance du Secteur Financier), the CSL (Chambre des Salariés) / LLLC (Luxembourg Life Long Learning Center) and the EST (Ecole Supérieure de Travail). Since recently the CNPD is also providing training on data protection for the students of a newly created professional baccalaureate (BTS) on cybersecurity in a Luxembourg high school.
 - o DaProLab (Data Protection Laboratory) workshops are another type of awareness event organized by the CNPD. The aim is to exchange knowledge, ideas, interpretations and views on a predetermined topic between data protection professionals. Past editions focused on the security of exchanges in the field of health, data protection impact assessments or data processing in the finance/insurance sector.
- The celebration of the CNPD's 20th anniversary on 1 December 2022 in the presence of many guests including Prime Minister and Minister of Communications and Media, Mr Xavier Bettel, Minister of the Interior and Minister for Gender Equality, Ms Taina Bofferding and the Chair of the EDPB, Dr Andrea Jelinek, gave the occasion to honor the CNPD's history, achievements and staff and to communicate broadly on the importance of data protection in today's world.

Guidelines

- Since 2020, the CNPD published or updated its guidance on the following topics:
 - o Data protection in the context of the Covid-19 pandemic
 - o The impact of Brexit on international data transfers

- o Cookies and other tracking technologies
- o Geolocation of vehicles made available to employees
- o Election campaigns and data protection
- The CNPD also released some information articles on data protection challenges regarding ransomware, artificial intelligence and the metaverse.

Compliance tools

- The CNPD launched in May 2022 its “GDPR-CARPA” certification scheme, the first certification scheme under the GDPR at the national and European level. GDPR-CARPA allows companies, administrations, associations and other bodies established in Luxembourg to demonstrate that their personal data processing operations comply with the GDPR. The first certification body authorized to issue the GDPR-CARPA certification was accredited by the CNPD in October 2022, followed by 2 other bodies accredited in 2023. In this context, the CNPD organized the launching conference “GDPR certification is coming to Luxembourg”.

With financial support from the European Commission the CNPD, in collaboration with the Luxembourg House of Cybersecurity and the National Cybersecurity Competence Center, is conducting the ALTO project (“DAta Protection ComPLiance Support TOolkit”). Its objective is to provide SMEs with a simple, intuitive and free self-assessment tool enabling them to integrate the GDPR obligations into their daily activities. The focus will be on the fundamental principles set out in the GDPR as well as on the reinforcement of the respect of individuals' rights in the context of the personal data processing envisaged and in progress. ALTO is aimed at all local SMEs that need to comply with the GDPR, both as data controllers and data processors. The product will have the potential to be used after adaption outside of Luxembourg.

7 Additional Policy Messages

In the previous GDPR report, the EDPB provided general policy messages, highlighting additional areas and topics that the EDPB considered worth mentioning. For example, the EDPB underlined the need to provide DPAs with sufficient resources, acknowledged the challenges of SMEs and addressed the topic of international transfers more in depth, among others.

*** 7.1 Would you like the future EDPB GDPR report to include an additional section on General policy messages?**

- Yes
- No

*** 7.2 Please add the topics and/or policy messages you would like to include in the EDPB report. Elaborate the reasons why, in your view, such topic should be included.**

1. Cooperation of DPAs with other authorities (competition, consumer, standardization, ethics ...) needs to be structured with regard to the interactions of GDPR with newly adopted EU regulations (DGA, DSA, DMA), EU regulations under preparation/adoption (IA Act, Data Act) and sector specific regulations emerging from the DGA (European Health data space EHDS,) and the European strategy for data. To avoid multiple and contradicting regulations, guidance and enforcement.
2. Support DPAs interactions with very small businesses, start-ups and SMEs and non-for-profit organisations to improve their awareness on privacy and data protection principles as defined within the GDPR. Stimulate systematic use of compliance tools such as privacy risk assessment to increase their maturity level by adopting a privacy-by-design/by-default attitude.
3. Foster education and training on data protection basics in the context of AI. The use of AI tools and especially generative AI tools will strongly amplify risks on personal data and privacy.
4. Develop general knowledge on AI in DPAs. In order to be prepared to face quickly upcoming challenges, DPAs will need to be able to recruit additional specific expertise in AI but also provide existing staff not having a technical background (lawyers) with basic knowledge on AI concepts as well as on other new technologies impacting their future work.

Contact

[Contact Form](#)