The right to lodge a data protection complaint: OK, but then what?

An empirical study of current practices under the GDPR

González Fuster, Gloria; Ausloos, J.; Bons, Damian; Bygrave, L.; da Rosa Lazarotto, Barbara; Drechsler, Laura; Gkotsopoulou, Olga; Hristov, Christopher; Irion, K.; Jasmontaite, Lina; Kroese, Charlotte; Lynskey, O.; Magierska, Maria

Publication date
2022

Document Version
Final published version

The right to lodge a data protection complaint: OK, but then what?
An empirical study of current practices under the GDPR

Data Protection Law Scholars Network (DPSN), June 2022.

Gloria González Fuster,[1] Jef Ausloos,[2] Damian Bons,[3] Lee A. Bygrave,[4] Barbara da Rosa Lazarotto,[5] Laura Drechsler,[6] Olga Gkotsopoulou,[7] Christopher Hristov,[8] Kristina Irion,[9] Lina Jasmontaite,[10] Charlotte Kroese,[11] Orla Lynskey,[12] Maria Magierska.[13]

This study was supported and commissioned by Access Now and reviewed by Estelle Massé.[14]

- Public version before design -

[1] Law, Science, Technology & Society (LSTS), Vrije Universiteit Brussel (VUB).
[2] Institute for Information Law (IViR), University of Amsterdam (UvA).
[3] IViR, UvA.
[4] Norwegian Research Centre for Computers and Law, University of Oslo.
[5] LSTS, VUB.
[6] FWO / LSTS, VUB.
[7] LSTS, VUB.
[8] IViR, UvA.
[9] IViR, UvA.
[10] LSTS, VUB.
[11] IViR, UvA.
[12] LSE Law School.
[13] European University Institute (EUI).
[14] Global Data Protection Lead at Access Now.

Executive summary

Access to data protection remedies constitutes a core element of the **enforcement of the General Data Protection Regulation** (**GDPR**).[15] Individuals confronted with a data protection infringement have the right to turn directly to the judiciary (Article 79 of the GDPR), but they have also **the right to lodge a complaint with a Data Protection Authority (DPA)** (Article 77 of the GDPR). They can lodge a complaint at the Member State of their habitual residence, of their place of work, or of the Member State of the place of the alleged data protection infringement. Data subjects also have the **right to an effective judicial remedy against the decisions of DPAs,** as well as in case of **lack of action** or **lack of information about the outcome or progress** of their complaint (Article 78 of the GDPR). Individuals can decide to mandate certain civil society organisations to represent them in front of DPAs, or in front of courts (Article 80 of the GDPR).

Data protection remedies are directly linked to two fundamental rights of the European Union (EU): the **right to the protection of personal data** and the **right to an effective judicial remedy**, enshrined in Articles 8 and 47 of the EU Charter of Fundamental Rights, respectively. Data protection remedies are at the crossroads of the exercise of individuals' rights and the obligations imposed on DPAs.

DPAs are independent authorities entrusted with the **consistent application of the GDPR**. They are obliged to **facilitate the submission of complaints**, notably '*by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication',* in line with Art. 57(2) GDPR. They are tasked with **handling** lodged complaints, and with **investigating, to the extent appropriate,** the complaints' subject matter.

This study examines current DPA practices related to their obligation to facilitate the submission of complaints, granting special attention to the connection between this obligation and the right to an effective judicial remedy against DPAs. It combines legal analysis and the observation of DPA websites, together with insights obtained from the online public register of decisions adopted under the 'one-stop-shop' mechanism.

The notion of **complaint** is not defined in the GDPR, which also does not elaborate on the meaning of the obligation '**to facilitate'** the submission of complaints. The exact meaning of '**to handle a complaint'** is equally not explicitly delimited by the GDPR – although by reference to Article 78 of the GDPR it emerges complaints shall result in an '**outcome**'.

In line with the case law of the EU Court of Justice, it can be understood as requiring from DPAs to examine the nature of individual complaints as necessary, with all due diligence. This obligation applies **to all complaints deemed admissible**. Some applied admissibility criteria, however, are currently elusive; some national practices seem to foresee admissibility criteria that go beyond GDPR requirements. There is also **fragmentation** and a certain **lack of clarity** regarding the exact moment in which it is possible for data subjects to exercise their right to an effective judicial remedy against a DPA, especially in case of absence of (timely) information by the DPA.

[15] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

There is also uncertainty surrounding the qualification of different types of outcomes marking the closure of a complaint file. This uncertainty is of particular relevance in the context of the **'one-stop-shop'** mechanism. When this mechanism applies, a complaint lodged by a data subject might end up being handled by multiple DPAs, which have to cooperate. If the final outcome of this procedure is a **rejection** or the **dismissal** of the complaint, it must be the DPA originally chosen by the data subject to lodge the complaint which has to adopt the final decision (Article 60(8) of the GDPR). The European Data Protection Board (EDPB), however, has recently announced that in its view this rule does not necessarily apply in cases in which the outcome is a so-called 'amicable settlement'.

The notion of '**amicable settlement'** has acquired significant importance recently, despite the fact that the GDPR only refers to it by connecting it to very specific cases linked to the one-stop-shop (in Recital 131). Procedures connected to a constellation of 'amicable solutions' can be viewed as connected to a more general trend favouring the handling of complaints with varied **degrees of intensity,** including what are often portrayed as '**light**', '**fast',** or '**soft**' procedures.

There is nevertheless much **opaqueness** in this regard, and the consistency of different national practices is unclear. The EDPB has been actively working discussing these issues, but available information on DPAs views and practices is limited. A recent framing of 'amicable settlements' as 'alternative dispute resolution' stands out.

Generally speaking, there is a lack of precise information on complaint-handling, including on the number of complaints lodged with DPAs. National registration and reporting practices appear to reflect and sustain **inconsistencies in national practices**, as well as the recurrent lack of clarity as to what can be expected by complainants after lodging a complaint.

To shed further light on existing practices concerning the facilitation of complaints submission by DPAs, this study reviewed a set of selected DPAs websites. The main findings of these observations are that although it is generally not difficult to find out how to lodge a complaint online, there is room for improvement regarding the effective facilitation of submission. Problems were notably identified in relation to **the possibility to lodge complaints from a different Member State**, touching upon the choices explicitly given to data subjects under Article 77 of the GDPR.

The research also revealed that DPAs generally **fail to give data subjects a clear picture** of **what to expect** from the submission of a complaint. This can be particularly problematic to the extent that it has an impact on the exercise of their right to effective judicial remedy against a DPA under Article 78 of the GDPR. There is also, in general terms, a lack of information on the very existence and possible consequences of the **one-stop-shop** mechanism. Equally, almost no information is provided to data subjects on their rights under **Article 80 of the GDPR**.

A review of the publicly available information on final one-stop-shop decisions reveals that **some DPA practices in relation to Article 60(8) of the GDPR are questionable.** In some cases, a final decision to reject or dismiss a complaint does not appear to have been taken by the DPA with which the complainant lodged the complaint, for unclear reasons. This kind of practice appears however to remain currently unchecked.

Overall, **the empirical research on DPA practices shows discrepancies that concern very fundamental aspects of the submission and handling of complaints, with potentially serious implications on the level of data protection in the EU.**

A number of possible **ways forward** are suggested. These include supporting best practices for the facilitation of complaint submission, providing more clarity about complaint-handling, further promoting the direct cross-border lodging of complaints, and better supporting the contribution of civil society organisations – for instance by the publication of a public register of entities falling under Article 80 of the GDPR.

The study's concluding remarks highlight the potential and challenges of research on access to remedies under the GDPR, notably by making a call for **more transparency from DPAs** in their discussions about this crucial component of GDPR enforcement.

List of figures

Introduction

The General Data Protection Regulation (GDPR)[16] heralded an improvement in the access to **remedies for data subjects** confronted with infringements of data protection law, in line with the recognition of data protection as a fundamental right of the European Union (EU). Access to data protection remedies constitutes a core element of GDPR enforcement.[17]

Under the GDPR, data subjects have the choice to either lodge a complaint with a Data Protection Authority (DPA)[18] or turn directly to the judiciary. Data subjects can also decide to mandate certain not-for-profit bodies, organisations, and associations to exercise these rights on their behalf, and thus represent them in front of DPAs, or in front of courts.[19]

If they wish to **lodge a complaint with a DPA,** data subjects have three possibilities: they can lodge the complaint with the DPA of the Member State of their habitual residence, with the DPA of the Member State of their place of work, or with the DPA of the Member State of the place of the alleged data protection infringement.[20]

Data subjects also have a **right to an effective judicial remedy against DPAs.** If the DPA receiving their complaint does not handle it, or if it does not inform the data subject within three months after the lodging of the complaint on its progress or its outcome,[21] the data subject can bring proceedings against the DPA – this must be before the courts of the Member State where the supervisory authority is established.[22] In addition, all natural persons have the right to an effective judicial remedy against a DPA's legally binding decisions '*concerning them'*.[23]

Data subjects can also, if they prefer, exercise their right to an effective judicial remedy by directly bringing proceedings against a controller or a processor.[24] They can do that either before the courts of the Member State where the controller or processor has an establishment, or, alternatively, before the courts of the Member State of the data subject's habitual residence.[25]

---

[16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.
[17] See Recital 129 GDPR: '*In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, ...*'.
[18] Hereafter also sometimes referred to as 'supervisory authority' or 'authority'.
[19] Art. 80(1) GDPR.
[20] Art. 77(1) GDPR.
[21] Art. 78(2) GDPR.
[22] Art. 78(3) GDPR.
[23] Art. 78(1) GDPR.
[24] There is a preliminary reference pending before the EU Court of Justice concerning the relationship between Art. 77 and Art. 79 GDPR: Request for a preliminary ruling from the Fővárosi Törvényszék (Hungary) lodged on 3 March 2021 – *BE v Nemzeti Adatvédelmi és Információszabadság Hatóság,* Case C-132/21.
[25] Unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers, in which case the only possibility is to bring proceedings in the Member State of the public authority; Art. 79(2) GDPR.

DPAs have the legal obligation **to facilitate the submission of complaints** by data subjects.[26] Concretely, DPAs must facilitate the submission '*by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication'*.[27]

Four years after the GDPR became applicable, it is necessary to analyse if its application is effectively translating into the anticipated improvement of access to data protection remedies. Against this background, this study examines **whether and how DPAs comply with their obligation to facilitate the submission of complaints**, and how the measures in place support or hinder data subjects' right to effective judicial remedy against DPAs.

To do so, the study first introduces the applicable GDPR rules concerning the submission of complaints, complaint-handling by DPAs, including complaints within the scope of the 'one-stop-shop' mechanism, and about the right to an effective judicial remedy against a DPA. Secondly, drawing on information available in the public domain, the study sets out how complaints are currently being handled by DPAs. Thirdly, it presents the findings of empirical research carried out concerning a number of selected DPAs – covering a representative sample of DPAs and Member States of different characteristics,[28] as well as insights obtained from the online public register of decisions adopted under the one-stop-shop mechanism. Finally, the study analyses these findings, and identifies possible options to improve access to data protection remedies and to promote effective GDPR enforcement.

1. Legal framework

Access to data protection remedies is crucial in light of both Article 8 and Article 47 of the EU Charter of Fundamental Rights (hereafter, 'the Charter').[29] **Article 8 of the Charter** enshrines the fundamental right to the protection of personal data.[30] The third paragraph of Article 8 explicitly recognises a special role for DPAs as a core component of such right, noting that compliance with data protection rules '*shall be subject to control'* by an independent authority.[31] **Article 47 of the Charter** establishes the EU fundamental right to an effective judicial remedy, noting that *'(e)veryone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal'*.

The right of data subjects to lodge a complaint with a DPA and the right to an effective judicial remedy appear explicitly connected in Recital 141 of the GDPR, which notes that data subjects have the right to an effective judicial remedy, in accordance with Article 47 of the EU Charter, *'where the supervisory authority does not act on a complaint, partially or*

[26] Art. 57(2) GDPR.
[27] Idem.
[28] Austria, Belgium, France, Germany, Greece, Italy, the Netherlands, Poland, Portugal, Lithuania, Spain.
[29] Charter of Fundamental Rights of the European Union [2012] OJ C326/391.
[30] Art. 8 EU Charter: '*Protection of personal data: (1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority'*.
[31] It is argued that failure by a DPA to *'consider the complaint of an individual in a meaningful way'* constitutes an interference with Art. 8 EU Charter: see Felix Bieker (2022), *The Right to Data Protection Individual and Structural Dimensions of Data Protection in EU Law*, Asser/Springer, p. 245.

wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject'.

The GDPR rules on complaints are at the crossroads between the rights granted to data subjects and the duties and obligations imposed on DPAs. These supervisory authorities are independent,[32] but they must nevertheless exercise their powers *'in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time'*.[33]

In addition, beyond rules limiting their competence in relation to their tasks and powers, the main duty of each DPA is to '*contribute to the consistent application of this Regulation throughout the Union'*.[34] As Recital 10 of the GDPR proclaims, the aim of the Regulation is to ensure the '*(c)onsistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data* (…) *throughout the Union'*.

1.1. Notion of complaint

The GDPR does not define the notion of **'complaint'**, as noted by the European Data Protection Board (EDPB)[35] in its *Internal Document 06/2020 on preliminary steps to handle a complaint: Admissibility and vetting of complaints*, of December 2020.[36] The EDPB has nevertheless stressed that complaints cannot be limited solely to infringements of a data subject right (as found in Chapter III GDPR). Rather, complaints can concern, more generally, any '*infringement of the Regulation by a processing of the complainant's personal data'*.[37]

In this internal document, the EDPB explicitly excludes from the notion of complaint any general requests about the GDPR made by individuals, as well as suggestions '*made by a natural person that he or she thinks that a particular company is not compliant with the GDPR as long as he or she is not among the data subjects'*.[38] Such suggestions of non-compliance by a controller or processor are referred to as **'tips'** in another EDPB document.[39]

The EDPB also distinguishes complaints from **'enquiries'**, which would be for instance *'a request for advice from a controller or processor on the implementation of data protection*

---

[32] Art. 52(1) GDPR: '*Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation'*; cf. also Art. 8(3) EU Charter, as noted.
[33] Recital 129 GDPR.
[34] Art. 51(2) GDPR.
[35] The EDPB was established by the GDPR with the prime task of ensuring its consistent application. It is an EU body composed of the head of one DPA of each EU Member State and of the European Data Protection Supervisor, or their respective representatives. Representatives of DPAs of European Economic Area (EEA) countries are also members but without voting rights.
[36] EDPB, *Internal EDPB Document 06/2020 on preliminary steps to handle a complaint: Admissibility and vetting of complaints*, adopted on 15 December 2020.
[37] Ibid., p. 3.
[38] Ibid., p. 4. Also explicitly excluded from the notion of complaint by the EDPB are '*cases without any reference to the processing of personal data such as disputes concerning exclusively commercial- or consumer protection matters such as a violation of the controllers general terms and conditions or violation of contracts'* (idem).
[39] EDPB, *Internal EDPB Document 02/2021 on SA duties in relation to alleged GDPR infringements,* Version 1.0, adopted on 2 February 2021, p. 14.

law or a request from a natural person for advice about how to exercise his or her rights'.[40] It should be noted however that occasionally the EDPB has used the term 'complaints' as able to encompass tips and signals – in this sense, it has stated that 'Article 77 complaints' would be one of the types of complaints that are submitted to DPAs.[41]

A preliminary reference currently pending before the EU Court of Justice concerns a question about the outcome of complaints, and whether the findings of DPAs following the lodging of complaints have the character of a 'decision' or a 'petition'.[42] According to the referring court, what is at stake is whether the judicial review of the outcome of complaints can be subject to a full substantive review by the courts or not.

1.2. The obligation to facilitate the submission of complaints

DPAs must **facilitate** the submission of complaints, notably '*by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication',* pursuant to Art. 57(2) GDPR.[43] This obligation has until now received very limited attention in the literature and from policy-makers.

The exact meaning of the verb 'to facilitate' in this context is not clear. Guidance by the EDPB in relation to the obligations imposed by the GDPR on controllers 'to facilitate' the exercise of data subject rights[44] can provide some insights on EU DPAs' views on the notion of 'facilitating'. In that context, the EDPB has highlighted that '*controllers should **undertake all reasonable efforts** to make sure that the exercise of data subject rights is facilitated',* adding that, '*for example, in case the data subject sends the request to an employee who is on leave, an automatic message informing the data subject about an alternative communication channel for its request could be a reasonable effort'*.[45]

Also in relation to data subject rights, the EDPB has noted that controllers '*should take special care to ensure that **people with special needs**, such as elderly people, children, visually impaired persons or persons with cognitive disabilities can exercise their rights, for instance by proactively providing easily accessible elements to facilitate exercise of these rights'*.[46]

DPA decisions elaborating on the meaning of a data controller obligation 'to facilitate' the exercise of data subject rights may also provide a sense of their interpretation of this notion. In January 2022, the Norwegian DPA stated that the obligation imposed on organisations to facilitate data subjects exercising their rights under the GDPR '*means that organisations must **allocate resources** and **have systems in place** to consider requests from private individuals'*.[47] A decision of the Belgian DPA, of February 2022, noted that according to its Litigation

---

[40] Idem.
[41] EDPB, *Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities*, August 2021, p. 10.
[42] Request for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Germany) lodged on 7 September 2021 – *FT v Land Hesse ('SCHUFA Holding')*, Case C-552/21.
[43] This obligation is established as a task of DPAs, the performance of which '*shall be free of charge for the data subject*' (Art. 57(3) GDPR).
[44] Cf. Art. 12(2) GDPR.
[45] EDPB, *Guidelines 01/2022 on data subject rights - Right of access*, Version 1.0, adopted on 18 January 2022, p. 21.
[46] Ibid., p. 44.
[47] Datatilsynet, decision of 14 January 2022, EDPBI:NO:OSS:D:2022:314, p. 4.

Chamber a data controller did not facilitate the exercise of the data subjects' rights insofar as an interface used could not be retrieved easily and at all times by the users, such as to allow them to amend their preferences in relation to data processing.[48]

1.3. The obligation to handle complaints

As noted, Recital 141 of the GDPR indicates that data subjects must have the right to an effective judicial remedy, in accordance with Article 47 of the EU Charter, *'where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject'*. However, the GDPR does not clarify how a DPA should '*act'* after receiving a complaint, and at which point it can be considered that a DPA did '*not act on a complaint',* opening the door to Article 78(2) of the GDPR.

The GDPR establishes the tasks of DPAs to '*handle complaints'* lodged by either data subjects or not-for-profit bodies, organisations, or associations (in accordance with Article 80), and to '*investigate, to the extent appropriate, the subject matter of the complaint'*.[49] This means that there is a general obligation for the complaints to be '**handled'**, and that the subject matter of the complaint shall be investigated '*to the extent appropriate'*.[50] In line with Recital 141, '*(t)he investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case'*.[51] There have already been instances of judicial review concerning the extent to which investigations had been conducted.[52]

The EU Court of Justice has underlined that pursuant to Article 57(1)(f) of the GDPR each DPA is required on its territory to handle complaints, adding that DPAs are '*required to examine the nature of that complaint as necessary'*,[53] and to handle complaints *'with all due diligence'*.[54] If a DPA does not apply all due diligence, it '*fails to deal'* with a complaint.[55] In this regard, the Court has emphasised that in order to handle complaints '*Article 58(1) of the GDPR confers extensive investigative powers on each supervisory authority'*,[56] and that –

---

[48] Gegevensbeschermingsautoriteit (GBA), Decision on the merits 21/2022 of 2 February 2022, Case number: DOS-2019-01377 (unofficial English translation available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf), p. 107.
[49] Art. 57(1)(f) GDPR.
[50] The EDPB appeared to conflate these two obligations when it referred to a '*prioritisation of complaints for handling to the extent appropriate*' in: EDPB, Contribution of the EDPB to the evaluation of the GDPR under Article 97, adopted on 18 February 2020, p. 11.
[51] In addition, Art. 58(4) GDPR establishes that the exercise of the powers conferred on DPAs, thus including investigative powers, 'shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter'.
[52] Cf., for instance, the judgment of the Spanish Audiencia Nacional (Sala de lo Contencioso) of 29 January 2019 (ECLI: ES:AN:2019:234), a case in which the court concluded that the Spanish DPA should have done more than merely blindly trust the allegations of the data controller before closing the file.
[53] Judgment of the Court of 16 July 2020, C-311/18, *'Schrems II',* ECLI:EU:C:2020:559, para. 109.
[54] Idem; '*by analogy, as regards Article 25(6) of Directive 95/46, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, para. 63'*. The EU Court of Justice had observed in the Schrems judgment (Judgment of the Court of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650) that, in the context of certain data transfers provisions of Directive 95/46/EC, when a data subject lodged a complaint with a DPA, it was 'incumbent upon the national supervisory authority to examine the claim with all due diligence' (para. 63).
[55] '*Schrems II',* para. 110.
[56] Ibid., para. 111.

when handling a complaint - the DPA is '*required to execute its responsibility for* ***ensuring that the GDPR is fully enforced with all due diligence****'*.[57]

Recital 129 of the GDPR offers general remarks about the tasks and powers of DPAs, mentioning some general principles, such as the fact that each DPA measure '*should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation,* ***taking into account the circumstances of each individual case****, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned'*.[58]

It is apparent that there is not full clarity as to what 'to handle a complaint' entails, and in which cases the dismissal of a complaint might constitute a form of handling, or rather lack of handling. Under Hungarian law, for instance, it is possible for the DPA to dismiss a complaint without examining it on its merits if the alleged infringement is of minor importance.[59] It would appear that in those cases the complaint has been examined to some extent (at least in order to determine its minor importance), but the decision is that it shall not be examined on its merits. Under Belgian law, a complaint might be deemed as deserving to move to the Litigation Chamber, only to be then filed without follow-up on the basis of a decision of the Litigation Chamber.[60] The Cyprus DPA may, according to national law, decide not to investigate a complaint, or discontinue an ongoing investigation, for reasons of public interest.[61]

The EDPB *Internal Document 06/2020* describes the steps to be undertaken by DPAs for the handling of complaints, including, as a first step, an admissibility check. The GDPR does not explicitly detail **admissibility criteria**.[62] The EDPB document notes that it can occur that a DPA receives a complaint *'that has to be rejected on admissibility grounds'*, mainly because: a) the subject matter is clearly not related to data protection, and thus the DPA is not competent; b) the complaint is manifestly unfounded or excessive pursuant to Article 57(4) of

---

[57] Ibid., para. 112. The judgment refers to a complaint about data transfers, but the described obligations of DPAs appear to apply generally to all complaints. The EDPB has in any case endorsed this reading: '*Even though the judgment relates to complaints in the context of transfer of personal data to a third country, the EDPB infers that the duty to review complaints with due diligence extends to all complaints, regardless of their subject matter'* (EDPB, *Internal Document 02/2021*, p. 10).

[58] This might be contrasted with the explicit reference to national procedural law in another sentence of the same Recital: '*Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation'*.

[59] Milieu, *Study on the national administrative rules impacting the cooperation duties for the national supervisory authorities: Questionnaire for the national supervisory authorities (Hungary),* EDPS/2019/02-07, February 2020, p. 3.

[60] Milieu, *Study on the national administrative rules impacting the cooperation duties for the national supervisory authorities: Questionnaire for the national supervisory authorities (Belgium),* EDPS/2019/02-07, February 2020, p. 7; it must be noted that the complaints 'filed without follow-up' are in any case classified as different from simply 'abandoned' cases (in French, 'abandonnés' v. 'classement sans suite'; in Dutch, 'afgesloten v. eigen sepot', Peter Van Rompuy, *Schriftelijke vraag nr. 7-287, aan de minister van Digitale Agenda, Telecommunicatie en Post, belast met Administratieve Vereenvoudiging, Bestrijding van de sociale fraude, Privacy en Noordzee*, Belgische Senaat, 17 januari 2020.

[61] Milieu, *Study on the national administrative rules impacting the cooperation duties for the national supervisory authorities: Questionnaire for the national supervisory authorities (Cyprus),* EDPS/2019/02-07, February 2020, p. 4.

[62] Some might be inferred from some GDPR provisions: for instance, it follows from the nature of most data subject rights that complaints about them will only be admissible if the data subject has first exercised them.

the GDPR;[63] or c) the complaint does not fulfil '*the formal conditions laid down by the Member State of the* [DPA] *which received the complaint'*.[64]

The EDPB has noted that, as regards the level of proof required to consider a complaint admissible, '*it is* ***necessary and sufficient*** *that the complainant provides a substantiated complaint',* meaning that *'the circumstances that allegedly constitute an infringement of the GDPR must be presented in a way that the supervisory authority will be able to investigate the case'*.[65] According to the EDPB, if '*the complainant presents circumstances that state a reason, why he or she considers that the processing of personal data relating to him or her infringes the Regulation, the complaint is substantiated'*, and DPAs should in any case '*take steps, if appropriate,* ***to clarify the unsubstantiated issues before dismissing*** *the complaint'*.[66]

Regarding admissibility requirements applicable in the Member State of the DPA, the *EDPB Internal Document 06/2020* observes that such national-level formal conditions could result from a variety of sources, ranging from a *'constitutional obligation to contact any administration in one of the official languages'* to '*the internal rule of the supervisory authority based upon respective legal provisions (such as, in some Member States, the obligation for the complainant to supply a proof of identity)'*, and encompassing '*other applicable legal requirements e.g. administrative procedure requirements of the relevant Member State'*.[67]

The document stresses that the applicable formal conditions to be taken into account for the admissibility of complaint are **those of the Member State where the complaint is lodged**. Thus, if the complaint is declared admissible and the 'one-stop-shop mechanism' applies, thus triggering the involvement of another DPA, such other DPA *'shall not re-examine the admissibility of the complaint'* based on formal aspects.[68]

The EDPB nonetheless suggests that when a complaint is to be rejected because it does not fulfil the necessary formal conditions, the rejecting DPA shall '*as a good practice and in alignment with its national law, first inform the complainant of the missing conditions in order to enable him or her to fulfil these conditions'*.[69] In any case, even if the complainant still does not provide all necessary elements for the complaint to be declared admissible, the DPA may inform other potentially concerned DPAs, something which '*may be particularly important when a complaint that is otherwise unsatisfactory for formal requirements reveals a serious infringement'*.[70]

---

[63] Art. 57(4) GDPR: '*Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request'*. The internal document argues that a complaint '*is unfounded when its subject matter falls within the scope of the GDPR but obviously does not justify an action from a supervisory authority*'. There is no explanation as to which complaints falling within the scope of the GDPR are to be regarded as not justifying any action by the DPA.

[64] EDPB, *Internal Document 06/2020*, p. 6.

[65] EDPB, *Internal Document 02/2021*, p. 14.

[66] Idem. This appears to be in tension with some statements such as the one from the Swedish DPA, according to which lodged complaints that are not *'completely filled out will be handled as tips'*, as stated here: https://www.imy.se/en/individuals/forms-and-e-services/file-a-gdpr-complaint/.

[67] Idem.

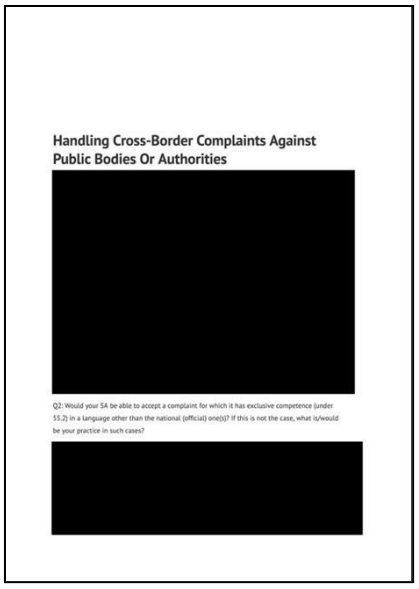
[68] Ibid., p. 7.

[69] Idem.

[70] Idem.

It must be noted that some Member States have expanded the possibilities for DPAs to reject complaints on grounds not foreseen under the GDPR. The Hellenic DPA, for example, may, according to national law, not only reject complaints which are manifestly unfounded, but also those that are manifestly vague, and those that 'shall be misused'.[71] Italian law foresees the restriction of the right of the data subject to lodge a complaint under Article 77 of the GDPR in a variety of cases, such as if the exercise of the rights may prove factually, effectively detrimental to the interests safeguarded by anti-money laundering provisions, or to the interests safeguarded by the provisions aimed to support victims of extortion.[72]

Some requirements and practices remain elusive. The EDPB compiled statements of DPAs on whether they would be able to accept a complaint for which the authority has exclusive competence in a language other than the national (official) one(s), but the version of the document made available to non-EDPB members after an access to documents request is significantly redacted.[73]


Handling Cross-Border Complaints Against Public Bodies Or Authorities

[redacted]

Q2: Would your SA be able to accept a complaint for which it has exclusive competence (under 55.2) in a language other than the national (official) one(s)? If this is not the case, what is/would be your practice in such cases?

[redacted]

*Figure 1 – First page of EDPB document "*Handling Cross-Border Complaints Against Public Bodies or Authorities (*without date*)

The visible answers reflect a significant level of unpredictability and heterogenous approaches.[74] The Danish DPA indicated it could accept complaints '*written in English (or in*

[71] See Art. 13(2) of Law No. 4624.

[72] Art. 2-undecies (Limitazioni ai diritti dell'interessato), Capo III, Codice in materia di protezione dei dati personali.

[73] EDPB, *Handling cross border complaints against public bodies or authorities,* document without date, probably dated 2021 (a request for mandate is mentioned in the Agenda of the 43rd EDPB meeting of 15 December 2020), Document 89 of request for access to documents 2022-19, submitted by *noyb* to the EDPB (documents obtained in April 2022). This document might be connected to a document referred to as EDPB Internal Document 05/2021 complaints against public bodies in the request for access to EDPB documents 2022/31 (cf. https://www.asktheeu.org/en/request/list_of_internal_documents#incoming-37148).

[74] A certain lack of predictability in some Member States has also been highlighted by the doctrine. It has been argued, for instance, that although a provision exists in Romanian law allowing for the submission of complaints in Romanian or English, considering that the Romanian Constitution provides that only Romanian is the official language in Romania, and noting the lack of specific rules on the language of the answers to be provided to complaints, it can be expected that complaints submitted in English with the Romanian DPA shall be responded

Danish and depending on the circumstances in Swedish or Norwegian)'.[75] The Slovenian DPA asserted that it would be able to accept complaints '*in another language that we understand (aside from Slovenian this is English, Croatian, perhaps some other languages depending on the staff's internal knowledge of a specific language)'*.[76] The Norwegian DPA ventured it could not be excluded that it would also accept complaints in languages other than the national official languages, English, Danish and Swedish.[77] The Slovak DPA stated it can only accept complaints lodged in Slovak language, and complaints in other languages shall be dismissed;[78] the Polish DPA also replied that it will not consider complaints not in Polish and lacking a Polish translation.[79] An authority identified as '*the FL DPA'* argued that the right to lodge a complaint with a DPA as enshrined in Article 77 of the GDPR '*cannot be made factually void in requiring a data subject to file a complaint in a specific language'*.[80]

The **existence of different administrative rules** that may impact the modalities of complaint handling also needs to be taken into account. The EDPB has emphasised that any '*differences in national procedural law can never lead to situations in which the principles of equivalence and effectiveness are undermined'*.[81] The European Free Trade Association (EFTA) Court also pointed out, in a 2020 judgment about the Article 77 of the GDPR, that national rules '*must not render practically impossible or excessively difficult the exercise of rights conferred by EEA law'*.[82]

In its *Guidelines 02/2022 on the application of Article 60 GDPR* the EDPB stressed that '*an interpretation of a given provision must not undermine the* ***effectiveness of EU law*** *and its principle of primacy in an area that has been regulated by the EU'*, in reference to the EU principle of procedural autonomy and its limits.[83] In this sense, it recalled that **the general principle of national procedural autonomy is limited by the EU principles of equivalence and effectiveness**.[84] Moreover, it explicitly pointed out that '*national regulations that contradict EU law must in principle remain unapplied',*[85] and recalled that '*the effects of national procedural regulations must not lead to limiting or hampering the cooperation under the GDPR'*.[86] This means, notably, that if national laws would undermine the effectiveness of the GDPR, they would need to be disapplied in this context.[87]

---

in Romanian (Marius Petroiu (2018), 'Romania: overview of the GDPR implementation', *European Data Protection Law Review* (EDPL), 4(3), p. 368.

[75] Ibid., p. 5.

[76] Ibid., p. 10.

[77] Ibid., p. 14.

[78] Ibid., p. 6.

[79] Ibid., p. 22.

[80] Ibid., p. 25.

[81] EDPB, *Internal Document 02/2021*, p. 12.

[82] Judgment of the EFTA Court of 10 December 2020, Adpublisher AG and J, and Adpublisher AG and K, Joined Cases E-11/19 and E-12/19, para. 45.

[83] EDPB, *Guidelines 02/2022 on the application of Article 60 GDPR, Version 1.0,* adopted on 14 March 2022, p. 2.

[84] As expressed by the EDPB, '*These principles stipulate that the applicable national rules must not treat an EU determined matter more unfavorably than purely national ones (equivalence*)' and that '*the application of national provisions must not significantly complicate or make it practically impossible to realise the purpose of the European legal standards (effectiveness)'* (EDPB, *Guidelines 02/2022*, p. 11).

[85] Idem.

[86] Ibid., p. 2.

[87] As an example of DPA decision to not apply some national provisions, see: Comissão Nacional de Proteção de Dados (CNPD), *Deliberação 2019/494*, 3 September 2019.

In addition, the EDPB '*highlighted that terms of EU law not making express reference to member state law must normally be given an* ***autonomous*** *and* ***uniform interpretation'***. It made this statement specifically in the context of a discussion of the situations that constitute a dismissal/rejection of a complaint, and the situations in which the lead supervisory authority '*acts on the complaint'* in relation to the controller.[88] **This means, concretely, that the meaning of 'to dismiss', 'to reject' or 'to act on' a complaint is not determined by national laws and practices, but by EU law.**

The EDPB compiled in a document DPAs' answers to the questions on their understanding of whether they have an obligation to investigate complaints.[89] The answers of some DPAs appear as partially redacted in the version of the document made available to non-EDPB members after an access to documents request (France,[90] Bulgaria,[91] Ireland);[92] the answer of the Dutch DPA is completely masked.[93]

1.4. Effective judicial remedy following the lodging of a complaint

Pursuant to Article 57(1)(f) of the GDPR, DPAs are obliged to '*inform the complainant of the progress and the* ***outcome of the investigation***[94] *within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary'*. Recital 141 includes very similar, but not identical wording. It states that '[t]*he supervisory authority should inform the data subject of the progress and the* ***outcome of the complaint***[95] *within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject'*.

Not all complaints lodged with a DPA will necessarily trigger a comprehensive, detailed investigation.[96] The EDPB has indicated that when a DPA '*decides not to investigate a complaint further, the complainant must be informed hereof and be provided with the rationale for concluding the investigation'*.[97] According to the Board, the outcome of a complaint *'could e.g. be an establishment of an* ***infringement****, that the parties to the complaint through the intervention of the* [DPA] *have* ***settled the case amicably*** *or, that the SA has* ***sent a letter*** *to the controller reminding it of its duties'*.[98]

The obligation imposed on DPAs to inform data subjects about the outcome of a complaint is also indirectly enshrined in Article 78(2) of the GDPR, which gives data subjects the right to

---

[88] Ibid., p. 3.
[89] Document 95 of request for access to documents 2022-19, submitted by *noyb* to the EDPB (documents obtained in April 2022).
[90] Ibid., p. 1.
[91] Ibid., p. 2.
[92] Ibid., p. 3.
[93] Ibid., p. 4.
[94] Underlined by the authors.
[95] Underlined by the authors.
[96] The EDPB has noted in this regard that it falls within the discretion of the DPA '*to assess and decide with all due diligence the extent to which specific investigative and corrective measures are appropriate, necessary and proportionate'* (EDPB, *Internal Document 02/2021*, p. 15).
[97] Idem. The EDPB also notes that the relevant *'reasoning may – depending on the type and complexity of the case – be kept rather short'* (ibid., p. 16).
[98] Ibid., p. 15. There is a preliminary reference pending before the EU Court of Justice about whether where a DPA finds that data processing has infringed a data subject's rights, the DPA must always take action exercising its corrective powers (however insignificant the infringement): request for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Germany) lodged on 14 December 2021 – *TR v Land Hessen*, Case C-768/21.

take the DPA to court if it fails to inform them about the outcome of a lodged complaint within three months.[99] Once informed about the outcome of the complaint they lodged with the DPA, data subjects will be in a position to consider whether they wish to exercise their right to an effective judicial remedy against the DPA's decision – to the extent that this is covered by Article 78(1) of the GDPR, which grants natural persons the right to an effective judicial remedy against a DPA's legally binding decisions '*concerning them'*.

The data subjects' right to an effective judicial remedy against DPAs under Article 78 of the GDPR encompasses what can be envisioned as two basic scenarios, described by the EDPB as, on the one hand, a right to the right to an effective judicial remedy against a legally binding decision of a DPA, and, on the other, *'against an 'inactive' supervisory authority'*.[100]

The first scenario, concerning a DPA that takes a decision that is contested, is further elaborated in Recital 143: each person should have an effective judicial remedy before the competent national court against a decision of a DPA '*which produces legal effects concerning that person'*, adding that such a decision *'concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority* ***or the dismissal or rejection of complaints'***.[101] In view of the EDPB, this Recital illustrates that the dismissal or rejection of a complaint must be regarded as '*a legally binding decision affecting the complainant'* in the sense of Article 78 of the GDPR.[102]

The second scenario concerns a DPA that does not handle a complaint and/or does not adequately inform the data subject, and is thus completely 'inactive' or at least not active enough in keeping the complainant duly informed for the purposes of Article 78.

Sometimes the line between the first and the second scenario is not manifestly evident. Under Dutch law, for instance, some DPA decisions not to handle a complaint are to be regarded as decisions by the DPA that can be appealed.[103] The legal qualification of the closure of a complaint is in any case under Dutch law dependent on whether it constitutes a request for the use of corrective powers: if not, the closure cannot be appealed, if yes, it is regarded as a rejection of the request, which is a decision that can be appealed.[104]

In relation to legally binding decisions adopted by DPAs, Recital 129 notes that '*(e)ach legally binding measure of the supervisory authority* ***should be in writing****, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure,* ***and refer to the right of an effective remedy****. This should not preclude additional requirements pursuant to Member State procedural law'*. The main reason justifying all these requirements is echoed in the final sentence of Recital 129, hinting at Article 78 of the GDPR: '*The adoption of a legally*

[99] The provision also refers to the need to inform the complainant three months after the lodging of the complaint, which, however, according to the EDPB, does not mean that the DPA must nor to inform the complainant repeatedly every three months (ibid., p. 12).
[100] EDPB, *Internal Document 02/2021*, p. 7.
[101] In some Member States, the possibility to access administrative remedies is also available, for instance by appealing to a higher level of decision-making within the DPA (cf. Spain).
[102] EDPB, *Internal Document 02/2021*, p. 12.
[103] Milieu, *Study on the national administrative rules impacting the cooperation duties for the national supervisory authorities: Questionnaire for the national supervisory authorities (Netherlands),* EDPS/2019/02-07, February 2020, p. 5.
[104] Ibid., p. 6.

binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision'.[105]

According to the information collected by the European Commission from Member States representatives, the majority of Member States comply with their obligations under Article 78 of the GDPR, but not all. Concretely, Finland and Sweden would not make available a judicial remedy, but only other types of legal remedies (via the Chancellor of Justice and the Parliamentary Ombudsman).[106] In April 2022 the European Commission launched formal infringement procedures against both (Finland[107] and Sweden)[108] for failure '*to fulfil their obligations as regards the right to effective judicial remedy for data subjects in certain cases'*.[109]

It is important to note that Article 78(2) of the GDPR does not prescribe an exact timeframe to complete the handling of complaints, although some national laws do have their own time requirements. These might derive from national data protection laws, or internal procedures, or general administrative law, and range in general terms from between one month and one year.[110] Some Member States provide for a suspension of the applicable time requirements when the one-stop-shop applies.[111]

Illustrating the diversity of rules in this regard, in Spain there is a six month deadline to react to some complaints, and in case of lack of decision before the expiry of this period the claimant may consider that the complaint has been resolved favourably by the DPA.[112] In Luxembourg, if an administrative body has not adopted a decision within three months of the

[105] The European Commission's Expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 discussed national interpretations of the notion of 'legally binding decision' under Art. 78 GDPR during its meeting of May 2021 (European Commission's Expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, *Questions for the GDPR/LED Member States Expert Group*, May 2021, p. 3).
[106] European Commission, *Implementation and transposition of Articles 85 and 78 GDPR and Article 53 LED: Overview of discussions with the members of the GDPR/LED expert group*, November 2021, p. 5.
[107] Infringement procedure INFR(2022)4010.
[108] Infringement procedure INFR(2022)2022.
[109] European Commission, *April infringements package: key decisions*, 6 April 2022.
[110] EDPB, *Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities*, op. cit., p. 22.
[111] See for instance, regarding Austria: Milieu, *Study on the national administrative rules impacting the cooperation duties for the national supervisory authorities: Questionnaire for the national supervisory authorities (Austria)*, EDPS/2019/02-07, February 2020, p. 3; Milieu, Study on the national administrative rules impacting the cooperation duties for the national supervisory authorities: Questionnaire for the national supervisory authorities (Netherlands), EDPS/2019/02-07, February 2020, p. 3, and Milieu, *Study on the national administrative rules impacting the cooperation duties for the national supervisory authorities: Questionnaire for the national supervisory authorities (Lithuania),* EDPS/2019/02-07, February 2020, p. 3, and presenting them as mutually alternative means of redress: the Codice in materia di protezione dei dati personali.
[112] EDPB, *Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities*, op. cit., p. 22. This concerns specifically complaints related to the exercise of data subject rights, and if the authority does not decide and notify the decision to the data subject after six months (cf. also: Alonso Ramón-Díaz (2022), 'La inadmisión a trámite de las reclamaciones presentadas ante la Agencia Española de Protección de Datos', Diario La Ley, No 9985, Sección Tribuna, 10 de enero de 2022, Wolters Kluwer).

introduction of a request, an implicit negative decision can be presumed.[113] France follows a similar approach.[114]

1.5. Decisions about complaints in the 'one-stop-shop'

The 'one-stop-shop mechanism' is a specific type of DPA cooperation procedure which needs to be followed in certain cases, and is mainly regulated by Article 60 of the GDPR. The EU Court of Justice noted in *Facebook Ireland Ltd* that '*the use of the 'one-stop shop' mechanism cannot under any circumstances have the consequence that a national supervisory authority, in particular the lead supervisory authority, does not assume the responsibility incumbent on it under Regulation 2016/679 to contribute to providing effective protection of natural persons from infringements of their fundamental rights* (…), *as otherwise that consequence might encourage the practice of forum shopping*'.[115]

Whereas DPAs are generally competent for the performance of the tasks assigned to them on the territory of their own Member State,[116] if the personal data processing at stake constitutes '*cross-border processing*'[117] the procedure established in Article 60 of the GDPR will apply, and the DPA '*of the main establishment*[118] *or of the single establishment of the controller or processor'* shall be competent to act as 'lead supervisory authority' in such procedure,[119] in principle.[120] This lead DPA will have to cooperate with all the other DPAs qualifying as concerned DPAs in order to take a decision, which will always include the DPA with which the complaint was lodged, if a complaint was lodged.

The one-stop-shop does not exclusively apply to cases initiated by the lodging of complaints, even if that is how most cases are launched in practice.[121] Most typically, a complaint is lodged with a DPA (sometimes called the 'receiving DPA', 'originating DPA', or with similar expressions, but lacking an official name) which will be different from the lead DPA, in procedures in which there may or may not also be other concerned DPAs.

By derogation to the general one-stop-shop procedure, if the concrete subject matter of a complaint concerns only processing activities of the controller or processor in the Member

---

[113] Milieu, *Study on the national administrative rules impacting the cooperation duties for the national supervisory authorities: Questionnaire for the national supervisory authorities (Luxembourg),* EDPS/2019/02-07, February 2020, p. 3.

[114] Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Art. 10.

[115] Judgment of the Court of 15 June 2021, *Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA, v Gegevensbeschermingsautoriteit*, Case C-645/19, ECLI:EU:C:2021:483, para. 68.

[116] Art. 55(1) GDPR.

[117] As defined in Art. 4(23) GDPR: '*cross-border processing' means either: (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.'*

[118] Cf. Art. 4(16) GDPR.

[119] Art. 56(1) GDPR.

[120] Unless *'the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State'*, in which case the derogation of Art. 56(2) GDPR applies.

[121] In this sense: EDPB*, First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities*, 2019. EDPB, *Annual report 2018: Cooperation and transparency*, 2019, p. 17; EDPB, *Annual report 2020: Ensuring data protection rights in a changing world*, 2021, p. 55.

State where the complaint was lodged, and if the matter does not substantially affect or is not likely to substantially affect data subjects in other Member States, the DPA with which the complaint was lodged shall be competent to handle the complaint. This derogation might be described as referring to '**local cases'**, or rather as one-stop-shop scenarios with a marked local dimension. Recital 131 further elaborates on these cases, stating that, in these cases, the DPA that originally received the complaint '*should **seek an amicable settlement** with the controller and, if this proves unsuccessful, exercise its full range of powers'*.

This mention of a possible 'amicable settlement' in Recital 131 is of particular interest, as there appear to be different readings regarding its significance. On the one hand, it is possible to read this reference as an acknowledgement or endorsement by the legislator of the general opportunity for DPAs to seek 'amicable settlements' (a notion which is nevertheless not defined). On the other hand, it is also possible to avoid such generalisation, emphasising that the reference appears in the GDPR only in a specific Recital, and only in reference to exceptional (local) derogations to the one-stop-shop procedure.

The EDPB *Internal Document 06/2020* examined **the notion of 'amicable settlement'**. It observed that this term is mentioned in Recital 131, and put forward that '*we could consider that the "amicable settlement" means the use of some'* of the DPA powers '*which **do not imply the use of corrective powers**'*.[122] Such use of some (non-corrective) powers would occur, for example, when '*a controller or processor accepts to provide any information requested by a supervisory authority to resolve a complaint'*, or when a '*controller abides by the request of the data subject after the supervisory authority asks it to do so'*.[123] On the contrary, in line with this internal EDPB document, there would be no 'amicable settlement' when the controller or processor refuse to do what they have been requested to do, or when the DPA exercises powers such as '*carrying out investigations in the form of data protection audits, obtaining access to all personal data, or obtaining access to any premises of the controller and the processing'*. [124]

When the general one-stop-shop procedure applies, Article 60(7) of the GDPR establishes that the lead DPA '*shall adopt* (…) *the decision…'*. This **decision** mentioned here is the decision concerning the outcome of the one-stop-shop procedure. It must be recalled that in the context of other provisions about complaints there is no explicit reference to the obligation of DPAs to specifically adopt a decision following a lodged complaint – as shown above, as a general task DPAs must handle complaints and investigate the subject matter at stake as necessary, and they also obliged to inform the data subject about the *outcome of the complaint*.

In any case, when the one-stop-shop applies, the lead DPA shall in principle, and pursuant to Article 60(7) of the GDPR, not only **adopt a decision** but also notify such adopted decision '*to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds'*.[125]

By derogation to this general rule, Article 60(8) of the GDPR foresees that if with the decision adopted by the lead DPA '*a complaint is dismissed or rejected, the supervisory*

[122] Ibid., p. 5.
[123] Idem.
[124] Ibid., p. 6.
[125] Art. 60(7) GDPR.

authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof'.[126] Exceptionally, then, if the final decision of the one-stop-shop procedure is going to be **to dismiss or reject a complaint**, it is not the lead DPA but the originating DPA (supposing they are not the same) that will adopt such a decision.

If the final decision concluding the one-stop-shop procedure is to dismiss or reject parts of a complaint, while acting on other parts on the complaint, Article 60(9) of the GDPR establishes that '*a separate decision shall be adopted for each of those parts of the matter',* and that the DPA with which was lodged the complaint will in any case '*adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof'.*[127]

The objective of these detailed rules is to make sure that any decision constituting the dismissal or rejection of a complaint is adopted by the DPA with which the data subject originally lodged the complaint. This is important because, in line with Article 78(3) of the GDPR, '*(p)roceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established'.*[128] If the data subject lodged a complaint with a DPA but then a decision dismissing or rejecting such complaint would be adopted by another DPA, the data subject would be obliged to bring proceedings against such decision in the Member State not of the DPA originally chosen by them, but another one.

The references in Article 60 of the GDPR to the 'dismissal' and 'rejection' of complaints have generated much uncertainty, as the GDPR does not define these notions, and Member States have a variety of procedures that might be perceived as somehow connected, but are not necessarily equivalent. These national procedures are directly relevant because, as noted by the EDPB, the decision at the end of the one-stop-shop procedure might be either '*the implementation **by way of a national decision** of the consensus reached under Article 60(6)*' of the GDPR, and/or '*the implementation **by way of a national decision** on the basis of the binding decision of the EDPB adopted under Article 65,*[129] *following the procedure provided under Article 65(6)*', and that the DPA adopting the decision '*will need to adjust the format to comply with its national administrative rules'.*[130]

The EDPB has looked into this issue and has interpreted, reading Article 60(9) jointly with Article 60(8) of the GDPR, that '*dismissal/rejection of a complaint as the outcome of an Article 60 procedure entails that the (part of the) final decision to be adopted **does not contain any action to be taken** in relation to the controller'.*[131] Thus, '*a decision dismissing or rejecting a complaint (or parts of it) should be construed as a situation where the LSA has*

---

[126] Art. 60(8) GDPR.
[127] Art. 60(9) GDPR, which also indicates: '*The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof'.*
[128] As also echoed in Recital 143: '*Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings before the courts in the same Member State'.*
[129] Art. 65 GDPR can apply in certain Art. 60 GDPR cases, in particular when there is a need for EDPB intervention for dispute resolution.
[130] EDPB, *Guidelines 02/2022,* p. 38.
[131] Ibid., p. 41.

found, in handling the complaint, that ***there is no cause of action*** *regarding the complainant's claim, and no action is taken in relation to the controller'.*[132]

It is not completely clear how this construal of the rejection and dismissal of complaints as instances in which the DPA handles the complaint but there is (eventually) no cause of action fits with the already mentioned Recital 143. The Recital clearly differentiates *'the exercise of investigative, corrective and authorisation powers'* by DPAs from the dismissal or rejection of complaints.[133]

The EDPB *Guidelines 02/2022 on the application of Article 60 GDPR* offer a noteworthy interpretation of Article 60(8) of the GDPR, and of the obligation it imposes on the DPA which received the complaint to '*adopt the decision and notify it to the complainant'* '*where a complaint is dismissed or rejected'*. According to the EDPB, this provision is **not applicable** '*in particular,* ***with the amicable settlement situation'***, described here as '*the situation where the case has been resolved to a satisfaction of a data subject, when the infringement alleged in the complaint has been identified by the LSA and when the complainant agreed to an amicable resolution of this complaint'.*[134]

In those cases, the EDPB considers that there is a '***demonstrated removal of the cause of action'***, meaning '*the complainant obtained the vindication of his/her rights through the intervention of the LSA towards the controller, which meanwhile met the terms of the complainant's claim'.*[135] As a consequence, the EDPB puts forward that these situations do not fall under Article 60(8) but under Article 60(7) of the GDPR,[136] and thus the lead supervisory authority shall be the one to adopt the decision, as opposed to the DPA with which the complaint was lodged.

Equally, the EDPB holds that there can also be other situations, *'that* ***do not fall within the amicable settlement constellation****'*, in which the intervention of the lead supervisory authority '*led the controller to stop the infringement and fully satisfy the complainant's claim'*, and in which Article 60(8) of the GDPR would not apply.[137] Again, it is difficult to perceive the congruity of this reading with the idea that there is dismissal or rejection if there is no use of investigative, corrective and authorisation powers, as it refers to an intervention of a DPA.

The EDPB acknowledges in any case that **this has an impact on the data subject's access to judicial remedy**, and in this context stresses that *'whenever this scenario may happen, it should be ensured by the* [lead supervisory authority] *via the complaint receiving* [supervisory authority] *that the complainant is duly informed on the positive achievement and on the envisaged outcome of the complaint and expresses no disagreement'.*[138]

---

[132] Ibid., p. 42.
[133] With the sentence: '*Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints'* (the 'or' indicating here that dismissal and rejection are something different from the exercise of the mentioned powers).
[134] EDPB, *Guidelines 02/2022*, p. 43.
[135] Ibid., p. 42.
[136] Ibid., p. 43.
[137] Idem.
[138] Idem.

As will be seen, understanding when exactly – and why - DPAs consider it appropriate to apply Article 60(8) of the GDPR as opposed to Article 60(7), or vice versa, is not always easy in practice.

2. Existing knowledge of current complaint-handling practices of DPAs

Having described the applicable legal framework, it is useful to now situate it within the broader background of policy, (known) DPA challenges and strategies, and to reflect on the availability and limitations of data about complaints and their handling.

2.1. Policy background

Directive 95/46/EC,[139] applicable until it was repealed by the GDPR in 2018, imposed on DPAs an obligation to '*hear claims'* lodged by persons or associations.[140] This did not lead, however, to harmonised practices in this area. In 2003, the European Commission noted for instance that for some DPAs it was '*a normal practice'* to hear claims by the '*opening of an administrative procedure that is closed by administration resolution further to a data subject's complaint'*, while for other DPAs the expression '*to hear claims'* did not necessarily require such action.[141]

When the European Commission presented its proposal in 2012 for what was to become the GDPR, a key objective was to ensure stronger enforcement, and to overcome '*fragmentation as well as inconsistent implementation and enforcement in different Member States'*.[142] This is echoed in Recital 7 of the GDPR, referring to the need for *'a strong and more coherent data protection framework in the Union,* ***backed by strong enforcement'***, and the fact that ***'[l]egal and practical certainty*** *for natural persons, economic operators and public authorities should be enhanced'*.

A specific concern of the European Commission in 2012 were the difficulties related to data protection enforcement via the courts. The Impact Assessment accompanying the proposed GDPR highlighted that *'(d)espite the fact that many cases where an individual is affected by an infringement of data protection rules also affect a considerable number of other*

---

[139] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

[140] Art. 28(4) of Directive 95/46/EC: *'4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim. Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place'*.

[141] European Commission, *Analysis and impact study on the implementation of Directive EC 95/46 in Member States*, 2003, p. 40. The analysis was partially based on a questionnaire sent to national authorities including questions such as '*is the opening of an administrative procedure at the discretion of your authority even if you have received a complaint from an individual? In case of affirmative response, we would appreciate to knowing what are the criteria on the basis of which your authority takes such decisions?*' (idem).

[142] EDPB, *Internal Document 02/2021*, p. 5.

individuals in a similar situation, in many Member States judicial remedies, while available, are very rarely pursued in practice'.

The European Commission hinted this appeared '*to be related to a general reluctance to bring an action to court, often related to the lack of information and the financial risk for the individual, when he/she is obliged to bear the costs of an unsuccessful claim for a judicial remedy, or when the damage is limited, e.g. in the case of unsolicited mails'.*[143] This problem was openly connected to the opportunity of allowing **associations** to represent data subjects in court cases.[144] Already in 2010 the European Commission had announced it wished to '*consider the possibility of extending the power to bring an action before the national courts to data protection authorities and to civil society associations, as well as to other associations representing data subjects' interests'.*[145] Also already at that time, researchers highlighted the importance of making sure that data subjects are *'able to obtain effective redress, as well as interim and permanent injunctions, in speedy, simple and cheap processes before competent, independent and impartial fora'*.[146]

In 2014, the EU Agency for Fundamental Rights (FRA) published a report on *Access to data protection remedies in EU Member States* which highlighted the importance for data subjects of being able to lodge a complaint with a DPA, notably in light of the lengthy, time consuming and complicated procedures and costs involved with judicial proceedings.[147] The report also stressed, however, that many individuals suffered from lack of information about procedures and insufficient knowledge of remedies.[148] Considering the input of many different actors, it recommended that what it called '*intermediary organisations'*, that is, civil society organisations, be supported and encouraged to function *'as a source of information, advice, legal assistance and representation'*.[149]

The European Data Protection Supervisor (EDPS) also voiced support for the representation of data subjects in front of DPAs and courts.[150]

These considerations eventually led the legislator to generalise the possible representation of data subjects by not-for-profit bodies, organisations and associations both in front of DPAs and in front of courts, in Article 80(1) of the GDPR.[151] This provision thus emerged as a

---

[143] European Commission, *Impact Assessment, Commission Staff Working Document accompanying COM(2012) 10 final, COM(2012) 11 final,* SEC(2012) 73 final, SEC(2012) 72 final, Brussels, 25.1.2012, p. 36.

[144] Only *'(s)ome businesses'* were reported to have '*argued that out of court settlements and mediation by DPAs can be more efficient than judicial redress'*, while a '*fairly large number of citizens'*, '*the DPAs and the EDPS'* were described as supporting what was to become the right to mandate an NGO, organisation or association to exercise the right to an effective remedy (ibid., p. 78).

[145] European Commission, *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee, and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union,* COM(2010) 609 final, Brussels, 4.11.2010, p. 9.

[146] Douwe Korff and Ian Brown (2010), *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments,* European Commission, p. 45.

[147] EU Agency for Fundamental Rights (FRA), *Access to data protection remedies in EU Member States*, 2014, p. 8.

[148] Idem.

[149] Ibid., p. 10.

[150] EDPS, *Opinion 3/2015, Europe's big opportunity, EDPS recommendations on the EU's options for data protection reform,* 2015, p. 6.

[151] Art. 80(1) GDPR has a broad scope, explicitly foreseeing that data subjects should be allowed to be represented in order to claim compensation (cf. Art. 82 GDPR); it is furthermore accompanied by a provision opening the door to action by not-for-profit bodies, organisations and associations without the mandate of a data subject. On this provision, see: Gloria González Fuster (2020), 'Article 80', in Christopher Kuner, Lee A.

major step forward to realising the potential of not-for-profit bodies, organisations and associations to contribute to strengthening the access to data protection remedies and GDPR enforcement.[152]

In March 2021, the European Parliament expressed its concern '*about the uneven and sometimes non-existent enforcement of the GDPR by national DPAs'*, noting that although numerous complaints had been lodged with them, *'only a very small share of submitted complaints has been so far been followed up'*.[153]

Also in 2021, the research and innovation services of the French DPA (Laboratoire d'Innovation Numérique de la CNIL) published a survey on the complainants that lodged complaints with it, who were asked to voluntary reply to questions. The survey results illustrated the importance of what was described as the '*procedural capital'* of the individuals concerned, that is, the knowledge about the procedure that they gather by actively lodging complaints. The research connected this to the fact that a relatively significant percentage of complainants appear to be '*repeat players'* as opposed to '*one shooters'*.[154]

2.2. Approaches to GDPR complaint-handling by DPAs

DPAs may face a variety of challenges that complicate the fulfilment of their tasks. A regular and common problem over the last years has been being understaffed and under-resourced,[155] and having to deal with overall increasing numbers of complaints from data subjects.

Increases in the number of complaints received have been particularly important for some authorities. The Irish DPA described a significant increase already in 2018,[156] in a report in which it declared that with the advent of the GDPR '*the DPC is no longer a data protection authority with a purely national focus; it has become a supervisory authority with an EU-wide remit, responsible for protecting the data privacy rights of millions of individuals across the EU'*.[157]

Reading the annual reports that DPAs are obliged to produce, it becomes apparent that **staff and resources problems have had an impact on the way in which they deal with**

Bygrave and Christopher Docksey (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary,* (Oxford University Press, 2020), pp. 1142-1152.

[152] On this subject, see for instance: Laima Jančiūtė (2019), 'Data protection and the construction of collective redress in Europe: exploring challenges and opportunities', *International Data Privacy Law*, Volume 9, Issue 1, February 2019, pp. 2–14.

[153] European Parliament, Resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application (2020/2717(RSP), paras. 12 and 13.

[154] See in particular Antoine Courmont (2022), '« On a beaucoup de droits, ok, mais pour les faire valoir, c'est compliqué » : les épreuves de l'exercice des droits', LINC/CNIL, 25 February 2022.

[155] Pointing out to a decline of budget allocation to DPAs: Irish Council for Civil Liberties (ICCL), *Europe's enforcement paralysis: ICCL's 2021 report on the enforcement capacity of data protection authorities*, 2021.

[156] Data Protection Commission (DPC) *Annual Report - 25 May - 31 December 2018*, 2019, p. 17.

[157] Ibid., p. 9.

complaints.[158] This has been visible since the very start of the application of the GDPR.[159] The Belgian DPA annual report for 2018, for instance, indicated that, due to understaffing, the authority had been obliged to make choices in the way it handled requests from data subjects.[160] A more recent document explained that depending of the amount of complaints received the DPA could resolve to decide on some complaints with what it described as the authority's 'light' procedure, but that, in case of an excessive amount of complaints, in the sense that the authority's Litigation Chamber would not be able to deal with in a reasonable timeframe taking into account its own resources, the same complaints shall be simply 'filed without follow-up'.[161]

The Covid-19 pandemic, and in particular personal data processing in this context, generated in some Member States an important increase of complaints, further increasing pressure on DPAs.[162]

In December 2021, the EDPB disclosed that although a majority of the DPAs were '*following-up on all complaints',* some authorities had reported '*that* ***they do not follow up on all complaints*** *received because of organisational, technical and human resource constraints'*. This specific acknowledgement did not concern GDPR complaints, but complaints related to infringements of Directive (EU) 2016/680[163] (known as the Law Enforcement Directive, or LED).

The possibility for DPAs to decide to deal only with some complaints, while ignoring others, seems openly incompatible with the GDPR. It is increasingly rare to witness DPAs openly support the lawfulness of such an approach.[164] Some have, in previous years, argued that it was up to them, based on their discretionary power, to decide whether to process a complaint

---

[158] Although these issues can have a negative impact broadly; the Hamburg DPA, in its 2021 report, stressed the need to be adequately equipped for its tasks, noting that lack of resources might negatively impact its independence (Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, *30. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit 2021*, April 2022, p. 7). Sometimes, in addition to limited staff and resources are highlighted other factors: in their report for 2019, the Austrian DPA refers also to the fact that the Austrian DPA heads the EDPB and an increased number of preliminary references from Austria to the CJEU with a data protection link, has led to issues with dealing with complaints timely. See: Datenschutzbehörde (DSB), *Datenschutzbericht 2019,* 2020, p. 68.

[159] See for instance: CNPD, *Relatório de atividades de 2017/2018*, 2019, pp. 3-4; CNPD, *Relatório de atividades de 2019/2020*, 2021, p. 19.

[160] Gegevensbeschermingsautoriteit (GBA), *Jaarverslag 2018*, 2019 (the report has no page numbers).

[161] In the French version: 'en cas d'afflux trop grand de plaintes que la Chambre Contentieuse ne saurait gérer dans un délai raisonnable compte tenu de ses moyens, la Chambre Contentieuse classera la plainte sans suite' (APD – Chambre Contentieuse, Politique de classement sans suite de la Chambre Contentieuse, op. cit., p. 4).

[162] In its report for 2021, the Austrian DPA reports that after the summer of 2021, they were flooded with complaints (3000 in December alone) for which they requested and were promised to receive additional staff. These complaints are linked to Covid-19 vaccination in Austria. For 2022, the Austrian DPA identifies as a challenge the timely handling of these complaints (noting also that they are legally obliged to deal with every complaint). See: Datenschutzbehörde (DSB), *Datenschutzbericht 2021,* 2022, p. 69.

[163] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 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, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119.

[164] Without prejudice to some occasional ambivalence. When in February 2021 the EDPB adopted the *Internal Document 02/2021 on SAs duties in relation to alleged GDPR infringements,* the European Commission '*raised that its understanding of the document is that it discusses the degree to which investigations will be conducted, without prejudice to the right for data subjects to complain under Art. 77 GDPR'*, according to the minutes of the EDPB meeting (EDPB, *45th Plenary meeting 2 February 2021 (Remote),* p. 3).

or not.[165] All seem however by now to be at least aware of the fact that they must assess each complaint individually – the Swedish DPA, for instance, acknowledged recently it was accepting this idea, in line with the orientation from the EDPB.[166]

The major trend at this moment is rather **to handle complaints with different degrees of intensity**. Specifically, some DPAs have been developing – sometimes building on specific national law, sometimes based on their own discretion, often inspired by other DPAs – ways of complaint handling sometimes described as '**fast**', '**light'** or '**soft**', reflecting the minimising of DPA involvement or a simplification of the procedure.

The Dutch DPA, for instance, acknowledged in its 2019 annual report that lack of resources and personnel, together with the increasing numbers of complaints, were resulting in problematic waiting times for data subjects wishing to lodge complaints.[167] In this context, it stated that it was deploying a variety of ways to handle complaints, including simply sending a letter to the data controller, or 'discussing'.[168] Its 2019 annual report mentions that it handles complaints in various ways, and that for a 'softer touch' it uses 'norm-transferring conversations' ('*normoverdragende gesprekken'*) (the term is not explained), letters, or mediation.[169] In 2020, the Dutch DPA reported that 1116 interventions were done based on complaints, an intervention being here a '**lighter form of investigation'**, for example a norm-transferring conversation with the organisation in violation of the GDPR, a letter to the organisation in which the DPA explains the norms, or a letter in which the authority requests more information from the organisation.[170] In parallel, the DPA also aimed at tackling its complaints backlog notably with an appropriate budget.[171]

In 2021, the Lithuanian DPA updated its complaints procedure, to include a 'settlement' or reconciliation procedure between the data subject and the controller in order to facilitate the effective exercise of the data subject's rights, referring to efficiency purposes.[172]

The 'fast-tracking', simplifying measures being implemented at national level by different DPAs can sometimes appear to be in tension with their obligation to actually handle complaints: it is unclear, in this regard, **how fast and simplified the handling of a complaint can be before it turns into a mere lack of handling**. DPAs sometimes emphasise that any 'alternative interventions' are deployed in full agreement with the wishes of the data

---

[165] Milieu, *Study on the national administrative rules impacting the cooperation duties for the national supervisory authorities: Questionnaire for the national supervisory authorities (Luxembourg),* EDPS/2019/02-07, February 2020, p. 5. There is still a certain ambivalence in the internal procedures of the Luxembourg DPA, which refer to decisions being taken *'in light of the characteristics of each complaint'*, but allowing the DPA to eventually decide to not handle a complaint by taking into account the total number of complaints and the available resources: Commission nationale pour la protection des données (CNPD), *Procédure relative aux réclamations devant la CNPD*, Art. 3.

[166] Integritetsskyddsmyndigheten (IMY), *Årsredovisning 2021*, 2022, p. 69.

[167] Autoriteit Persoonsgegevens (AP), *Jaarverslag 2019*, p.13.

[168] Ibid., p.11.

[169] Ibid., p. 13.

[170] Translations by the authors. Idem.

[171] AP, *Jaarverslag 2020*, 2021, p. 17.

[172] Valstybinės Duomenų Apsaugos Inspekcijos, *2021 Metų Veiklos Ataskaita*, 2022 m. kovo 7 d. Vilnius, p. 13; Valstybinės duomenų apsaugos inspekcijos direktoriaus 2021 m. kovo 2 d. įsakymas Nr. 1T-20 (1.12.E) 'Dėl Valstybinės duomenų apsaugos inspekcijos nagrinėjamų skundų nagrinėjimo tvarkos aprašo patvirtinimo', Skyrius V (Order of the Director of the State Data Protection Inspectorate No 1T-20 (1.12.E) of 2 March 2021 'On the Approval of the Description of the Complaints Handling Procedure of the State Data Protection Inspectorate', Chapter V).

subject.[173] It is unclear however how such wishes are ascertained; it would for instance be a problem if, in exchange for a promise of quick handling, data subjects were nudged into giving up on the full extent of their rights as granted by the GDPR.

Moreover, the fragmentation of practices triggers questions as to whether they are compatible with the **consistent application of the GDPR** throughout the EU. The Dutch DPA, for instance, explained in a 2018 document on its policy on the prioritisation of complaints that it follows a pragmatic approach, and that, when pertinent, it might for instance follow up a complaint by making a phone call to the data controller, trying to settle the case in such a manner.[174] This concerned what the Dutch DPA presented as a possible 'focus on mediation' as a legitimate way of handling a complaint.[175] This open reference to 'mediation' triggers the question of what is the consistency between this practice and the Belgian system according to which data subjects may *either* submit a request for mediation *or* a complaint. Allegedly, in circumstances in which a data subject has such the choice between mediation and complaint, and deliberately submits a complaint, it might not be appropriate for a DPA to handle their complaint as a request for mediation.[176]

Some inconsistencies between national practices, if at odds with the objectives of the GDPR, might be unlawful as such. In addition, they can result in problematic situations in one-stop-shop procedures – for instance, following the example, if a data subject submits a complaint in Belgium which is later treated as a request for mediation by the Dutch DPA.

The French DPA also has its own 'fast handling' ('*traitement rapide'*), which it has been applying to a great number of complaints[177] – approximately 40% of the complaints received in 2021.[178] This fast handling typically consists in sending information to the complainant, for instance about their rights, the obligations of data controllers, or other institutions able to help them.[179]

The trend towards 'fast', 'light' or 'soft' handling of complaints can be connected to the notion of '**amicable settlements'**, an expression already discussed above in relation to the GDPR, but which beyond it can have different meanings and implications depending on the context.[180]

---

[173] In this sense, AP, *Jaarverslag 2018*, 2019, p. 16 (referring to the complainant's wishes as guiding factor).
[174] AP, *Beleidsregels Prioritering klachtenonderzoek*, 2018, p. 5.
[175] Ibid., p. 7.
[176] It can occur that the Belgian DPA decides to 'file without follow-up' a complaint that had been deemed admissible, while at the same time recommending to the data subject to file a new request, but this time for a mediation. This notably happened in a case on which eventually had to decide the Tribunal de première instance francophone de Bruxelles (2021/2476/A): following the explicit advice of the DPA, the data subject accepted the filing of the lodged complaint and introduced instead a request for mediation, only to be informed months later that the mediation had failed, and the problem was thus finally not solved. The court ruled against the DPA for its inappropriate handling of the mediation request, illustrating that DPAs also have certain obligations in relation to procedures that do not fall under Art. 77 GDPR (judgment available here: https://noyb.eu/files/GDPRhub/Trib.%20Civ.%20Bruxelles%20-%202021_2476_A.pdf).
[177] For instance, to 5.620 complaints in 2019 (CNIL, *40e Rapport annuel 2019 : Protéger les données personnelles, Accompagner l'innovation, Préserver les libertés individuelles,* 2020, p. 81).
[178] CNIL, *Rapport annuel 2021 : Protéger les données personnelles, Accompagner l'innovation, Préserver les libertés individuelles,* May 2022, p. 41; it is not completely clear if all of the 5.848 complaints handled through the 'fast procedure' in 2021 were submitted in 2021.
[179] Idem.
[180] As noted in EDPB, Info Note: Cooperation subgroup, Outline – The practical implementation of the amicable settlement*, 25 September 2019* (Document 34 of request for access to documents 2022/27, submitted by Johnny

An EDPB poll among its members found that almost half of the respondents considered that 'amicable settlements' were possible in their national legislation (45%, 11 votes).[181] In the poll results as shared by the EDPB in response to an access to documents request, the names of the 'voters' had been masked (see Figure 2). According to the EDPB *Guidelines 06/2022 on the practical implementation of amicable settlements*, a total of 14 DPAs have indicated that amicable settlements are not possible in accordance with national legislation.[182] Previously, in 2020, the EDPB had proclaimed in its written input submitted for the European Commission in the context of the evaluation of the GDPR that only nine DPAs '*did not make use of amicable settlements'*.[183]

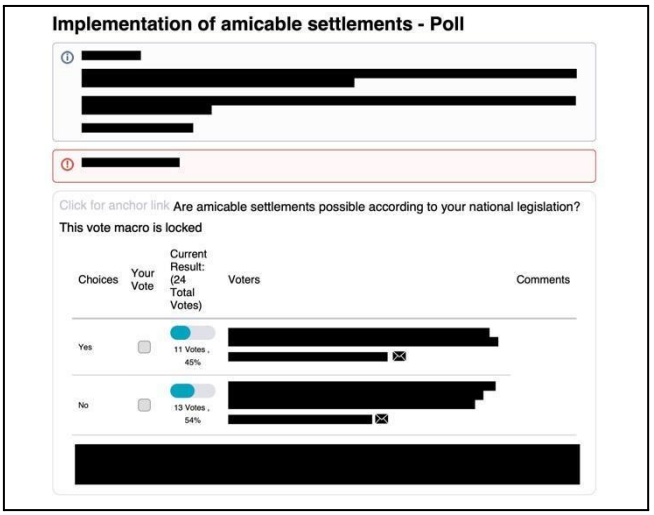


Figure 2 – EDPB Implementation of amicable settlements – Poll (without date)

Another EDPB document appears to compile DPA answers to questions about the rules applying to 'amicable settlements', but it was only shared by its services after being heavily redacted (see Figure 3).[184] Only the answers of three DPAs are at least partially accessible, from Liechtenstein, Hungary, and Finland.

Ryan to the EDPB (documents obtained in May 2022)), the notion of 'amicable settlement' as it can be found in some Member States 'might differ substantially from the amicable settlement mentioned in Recital 131' (p. 1).

[181] EDPB, *Implementation of amicable settlements - Poll,* document without date, Document 90 of request for access to documents 2022-19, submitted by *noyb* to the EDPB (documents obtained in April 2022).

[182] Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Greece, Malta, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden (EDPB, *Guidelines 06/2002 on the practical implementation of amicable settlements*, p. 22).

[183] EDPB, *Contribution of the EDPB to the evaluation of the GDPR under Article 97*, adopted on 18 February 2020, p. 33.

[184] EDPB, Document 91 of request for access to documents 2022-19, submitted by *noyb* to the EDPB (documents obtained in April 2022).

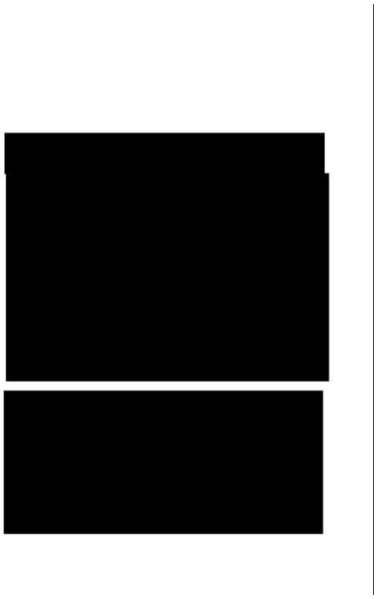


Figure 3 - EDPB document 91 of access to documents request 2022-19 (untitled, without date)

The Liechtenstein DPA explains that in line with its national procedural law a settlement agreement has the judicial effect of a formal binding decision, and that in case of '*amicable settlement involving a formal settlement agreement of the parties'* there will be no further formal binding decision by the DPA to close the case.[185] The authority notes also, however, that it can be that after an amicable settlement the complainant withdraws the complaint, or that the complaint eventually ceases to be a complaint and becomes a query, in which cases there would be no formal decision.[186]

The Hungarian DPA describes two scenarios in which an amicable settlement is conceivable. The first refers to a settlement in the context of the '*data protection administrative procedure'*, which would require approval by the DPA to be valid.[187] The second is described as some form of an amicable settlement in a broader sense, whereby a case is closed '*amicably'* if the data controller complies after communication with the DPA.[188] The authority notes that this has an impact on the right to an effective judicial remedy, but clarifies that it *'does not deem this controversial'* because this would not apply to formal complaints, but to inquiries.[189]

The Finnish DPA indicates that it has not identified any provisions in Finnish administrative law that would require the authority to take a binding decision in case of 'amicable settlement'.[190] The DPA uses the term to refer to the cases where the complainant is satisfied with the actions taken by the controller, and the complaint '*could be deemed as withdrawn'*.[191]

In its annual reports, the Irish DPA repeatedly celebrates the possibility provided under Irish law to endeavour to resolve complaints 'amicably', and it provides examples presumably

[185] Ibid., p. 15.
[186] Idem.
[187] Ibid., p. 18.
[188] Idem.
[189] Idem.
[190] Ibid., p. 21.
[191] Idem. According to the EDPB, *Guidelines 06/2002 on the practical implementation of amicable settlements*, amicable settlements are actually not possible in Finland (p. 22).

illustrating its advantages. The Irish DPA connects its emphasis on amicable resolution to a means of '*doing more, for more'*.[192] There are many ways in which a complaint might be amicably resolved, according to the Irish DPA: '*in some cases, this could involve **a gesture** on the part of the data controller, or the issuing of **an apology**, but equally a complaint might also be resolved through the clarification of an issue to the satisfaction of both parties'*.[193]

The Irish DPA actually conceives of complaints as essentially broken into three categories, depending on their suitability for amicable resolution: complaints that can be handled with ***'fast-track amicable resolution'***, involving minimal additional contacts between data controller and data subject;[194] complaints that have potential for amicable resolution, but only with a '*higher number of iterative contacts'*, and complaints lacking real potential for amicable resolution within a reasonable time period.[195] In any case, according to the Irish DPA under current Irish law it is not obliged to take a '*formal, statutory decision*' regarding each complaint.[196] When '*an amicable resolution is successfully achieved, a complaint will be deemed to be **withdrawn**'*.[197] A specific provision in Irish law establishes that a notification to the complainant of the fact that their complaint is deemed to be withdrawn is to be regarded as informing the complainant about the outcome of the complaint,[198] echoing Article 77(2) of the GDPR.

Some national 'fast-tracking' procedures appear to be very similar but cannot be conflated. The Spanish DPA has in recent years extensively relied on what it calls the '*traslado'* or transfer of complaints, consisting basically in reaching out to data controllers or processors after the reception of a complaint, with the objective of speeding up the resolution of the matters at stake. In its 2021 annual report, the Spanish DPA celebrates this practice noting this very simple 'transfer' can lead to either solving the complaint, or the gathering of information allowing it to clarify that no infringement of data protection rules has taken place.[199] The practice is explicitly connected by the DPA in its annual report to a provision of the Spanish law specifying the GDPR[200] which, however, is about the possibility to **declare inadmissible** complaints if the controller or processor, having been warned by the DPA, adopt the necessary corrective measures, and under certain conditions. Therefore, this national provision is not related to the handling of complaints, but to a step allowing for the rejection or dismissal of the complaint prior to handling – that is, the admissibility stage. It seems that when complaints are stopped after the 'transfer' stage, and thus prior to handling,

---

[192] DPC, *Annual Report 2021,* 2022, p. 18; this connects to the general strategy of '*doing more for more people'* (ibid., p. 10).
[193] Data Protection Commission (DPC) *Annual Report - 25 May - 31 December 2018*, 2019, p. 23.
[194] '*Of the 3,564 complaints concluded by the DPC in 2021, 463 of those complaints were concluded by fast-track amicable means'* (DPC, *Annual Report 2021*, p. 24.
[195] Section 109(2) of the Irish Data Protection Act 2018 2018 refers to a reasonable likelihood of amicable resolution within a reasonable time ('*The Commission, where it considers that there is a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint, may take such steps as it considers appropriate to arrange or facilitate such an amicable resolution'*).
[196] DPC, *Annual Report - 25 May - 31 December 2018*, 2019, p. 31.
[197] In accordance with Section 109(3) of the Data Protection Act; see: DPC, *One-Stop-Shop Cross-Border Complaint Statistics, 25 May 2018 – 31 December 2021*, 2022, p. 11.
[198] Cf. '*For the purposes of subsection (2)(b), the Commission shall be taken to have informed a complainant of the outcome of the complaint concerned where it gives the complainant a notice under section 109 (6) or, as the case may be, section 116',* Section 108 Data Protection Act 2018, subsection (3).
[199] Agencia Española de Protección de Datos (AEPD), *Memoria anual 2021*, 2022, p. 131.
[200] Art. 65 of the Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales – more specifically, this concerns Art. 65(3).

the Spanish DPA does not consider itself obliged to inform the data subject about any outcome, as formally there has been no admitted complaint.[201] Regardless of whether the underlying issue could be resolved this way, the compatibility of such a reading with Article 77 and Article 78 of the GDPR is highly questionable.

The EDPB has stated that '*it appears that amicable settlements generally refer to* ***alternative dispute resolutions*** *through proceedings that result in the cordial closure of a case'*, encompassing procedures ranging '*from party-to-party negotiations to formal mediations and even facilitated conciliation practices'*.[202] There is not much evidence in the literature that would confirm such a widespread framing by DPAs of complaint-handling as alternative dispute resolution.[203] The GDPR itself refers to the possibility to foresee *'**out-of-court proceedings and other dispute resolution procedures** for resolving disputes between controllers and data subjects with regard to processing'* only in the context of codes of conduct, and adding that such proceedings and procedures shall be *'without prejudice to the rights of data subjects pursuant to Articles 77 and 79'*.[204]

Coming back to possible ways of approaching complaints, some DPAs have connected the threshold of demands for the submission of complaints with the problem of having to deal with (too) many demands. In this sense, the 2019 annual report of the Belgian DPA indicated that the Litigation Chamber, taking into account what it described as a low threshold of accessibility of the complaints procedure, had decided to close certain cases, without any further action, for reasons of opportunity.[205] This concerns the already mentioned practice of 'filing without follow-up', which according to the Belgian DPA can occur when complaints do not meet the authority's priorities.[206]

From another perspective, improving the system for **online submission of complaints** appears to have an impact on the number of complaints, which would appear to increase, while at the same time facilitating and speeding up the follow up by the DPA.[207] The usefulness of online submission procedures became particularly visible with the Covid-19 pandemic, as some DPAs experienced delays in handling complaints received via letter, due to home-working of the staff.[208]

An appropriate system for the submission of complaints could help DPAs address the problems related to receiving significant numbers of non-admissible complaints, as online forms allow for better guidance during the submission.[209] The Irish DPA, for instance,

---

[201] AEPD, *Memoria anual 2021*, 2022, p. 79.
[202] EDPB, *Guidelines 06/2002 on the practical implementation of amicable settlements*, p. 6.
[203] Cf., making rather a link between alternative dispute resolution and compensation claims (and recalling the connection between alternative dispute resolution and the Safe Harbour Principles): Damian Clifford and Yung Shin Van Der Sype (2016), 'Online dispute resolution: Settling data protection disputes in a digital world of customers', *Computer Law & Security Review*, Vol. 32, Issue 2, pp. 272-285.
[204] Art. 40(2)(k) GDPR.
[205] GBA, *Jaarverslag 2019*, 2020, p. 27.
[206] Autorité de Protection des Données (APD) – Chambre Contentieuse, *Politique de classement sans suite de la Chambre Contentieuse,* 18 June 2021, p. 3.
[207] CNPD, *Relatório de atividades de 2019/2020*, p. 17. The report for 2017/2018 highlighted the necessity to improve technology and modify the way users accessed the DPA's website; the report 2019/2020 shows data that demonstrate that the creation of a modern website along with new forms for complaints increased citizens' participation.
[208] Datenschutzbehörde (DSB), *Datenschutzbericht 2020,* 2021, p. 60.
[209] In this sense: AEPD, *Memoria anual 2018*, 2019, p. 62.

laments that people complain to the DPC about matters where the concern is not a data protection issue.[210]

For some DPAs a key challenge in relation to complaints appears to be national administrative law and particularly demanding procedural requirements, that generate certain difficulties especially in relation to cooperation through the one-stop-shop.[211]

Finally, some DPAs appear to seek to limit the number of admissible complaints by increasingly relying on the possibility to reject complaints because they are considered excessive requests, based on the frequency of complaints per person.[212] This is connected to Article 57(4) of the GDPR, which refers to the possibility of refusing to act on a request (or, alternatively, charge a reasonable fee) in case of requests[213] which are manifestly unfounded or excessive, in particular because of their repetitive character.

There have been some court cases at national level connected to DPAs lack of handling.[214]

2.3. Counting complaints

Data about lodged complaints is currently available mainly only via the DPAs, which have **varied registration and reporting practices**. The GDPR does not require the existence of an EU-wide system of reporting data on complaints filed with the DPAs, nor does the EDPB consolidate national reporting data. Other available sources are rare.[215] Inconsistencies between DPAs in defining what constitutes an admissible complaint, and in the subsequent handling practices, exacerbate the deficiencies related to the availability of EU-wide comparable data.

---

[210] See, e. g., mentioning '*a myriad of every-day exchanges, a large proportion of which do not engage any issue of data protection at all, are nonetheless presented on the basis that the application of data protection rules are central to their resolution'*: DPC, *Annual Report 2021,* 2022, p. 6.

[211] In their report for 2018, the Austrian DPA mentions several legal challenges linked to the interaction of Austrian administrative law and the GDPR (DSB, *Datenschutzbericht 2018,* 2019, pp. 64-65). In their report for 2019, the Austrian DPA notes as a specific challenge for cross-border proceedings involving other Member States, the difficulty of combining diverging rules for the administrative proceedings (DSB, *Datenschutzbericht 2019,* 2020, p. 68).

[212] Cf. report of 2021 of the Austrian DPA, in which it provides a definition of excessive as in any case fulfilled if the same complainant brings more than two complaints a month for a duration of 12 months and thus 24 complaints per year (DSB, *Datenschutzbericht* 2021, p. 15).

[213] In the French version, '*demandes'*; in the German version, '*Anfragen'*.

[214] The report of the Austrian DPA for 2018 mentions five cases where there was a complaint to the administrative court about inaction of the DPA. It also explains that one of those was dismissed as the Austrian DPA was not required to act. It does not mention what happened to the other cases and provides no further details on them (DSB, *Datenschutzbericht 2018,* p. 43). For 2019, the Austrian DPA reports that 31 complaints were made to the administrative court because of inaction ('*Säumnisbeschwerde*'). There are no details how any of these complaints ended. The summaries of decision of the highest administrative court include one case concerning a complaint about inaction predating the GDPR, where the court found that the Austrian DPA failed to reject clearly the complaint because they were not yet competent (DSB, *Datenschutzbericht 2019,* 2020, p. 42 and pp. 60-61).

[215] The European Commission reported in 2012 that *'(*b*)ased on information from 20 Member States, there were 54,640 complaints concerning (potentially) unlawful processing of personal data or breaches of data protection rights in the EU in 2009'*, but this was based on ('(i*)nformation gathered via a survey by GHK consulting'* in the framework of a study not made publicly available, thus rendering impossible the interpretation of such data) (SEC(2012) 72 final, p. 29).

The **number of complaints made by data subjects** was nevertheless explicitly mentioned as an indicator of results and impact, to be periodically evaluated and used to monitor the implementation of the law in the proposal for the EU data protection reform.[216]

Data about complaints is typically made available by DPAs in their annual reports. Some of these annual reports include extensive and detailed figures about complaints, and many of them are, generally speaking, highly informative. A recurrent problem, however, is the lack of clarity about how some complaints are measured.

For instance, it is typically not clear if reported complaints include or exclude complaints that were submitted but eventually declared inadmissible, as well as how admissible but withdrawn complaints are counted (if they are counted), including those 'deemed withdrawn' due to an amicable settlement.[217] If the withdrawn complaints are counted as complaints, it is unclear if they are counted as 'concluded' complaints. Very often, it is unclear which are the periods to which the different events quantified relate, leading to situations such as the Spanish DPA claiming in its 2021 annual report that it **solved 101% of complaints**.[218]

The annual reports of the Irish DPA provide information on the number of complaints received and 'concluded'.[219] The Irish DPA also provides separate data on the number of one-stop-shop procedures in which it is involved as lead DPA, how many as a concerned authority, and how many have been 'concluded'.[220] The term 'concluded', however, is not defined.

The Austrian DPA distinguishes in all its annual reports since 2018 the complaints ended with a closing of procedures ('*Einstellung*') and those ending in a decision ('*Bescheid*').[221] It is unclear if all would fall under 'concluded', or only those ending in a decision.

The reports of the Hamburg DPA provide information about received *written* submissions, encompassing both data protection and freedom of information issues.[222] Among these are identified the number of data protection complaints, defined as a written submission with which data subjects turn to the Hamburg DPA with a claim that their GDPR rights have been infringed.[223] The Hamburg DPA does not clarify if it reports on all lodged complaints, or only those that were found to be admissible. As a matter of fact, it is not possible to understand, by reading the annual report, what happened to the complaints. More granular information is only provided for the complaints that led the DPA to exercise its corrective powers under Article 58 of the GDPR.

---

[216] SEC(2012) 72 final, p. 103.
[217] This is not clear, for instance, reading the available annual reports (post-GDPR) of the Dutch DPA.
[218] AEPD, *Memoria anual 2021*, 2022, p. 79.
[219] Including on how many of the 'concluded complaints' date from previous years, although not specifying the year in which those complaints were lodged.
[220] See e. g. DPC, *Annual Report 2021,* 2022, p.26.
[221] DSB, *Datenschutzbericht 2018,* 2019, pp. 10-11; DSB, *Datenschutzbericht 2019,* 2020, pp. 9-10; DSB, *Datenschutzbericht 2020,* 2021, pp. 9-10; DSB, *Datenschutzbericht 2021,* 2022, pp. 8-9.
[222] For 2021, see p. 134 and ff.
https://datenschutz-hamburg.de/assets/pdf/30._taetigkeitsbericht_datenschutz_2021.PDF.
[223] With a reference to Art. 77 GDPR.

In the Belgian DPAs annual reports, it appears that complaints that were regarded as inadmissible are also reported as handled complaints.[224] Sometimes the Dutch DPA separates 'handled' complaints into 'invalid', 'valid', and 'no verdict/withdrawn/amicable arrangement/other way of handling'.[225] It is unclear what is the exact relation between all these terms – supposedly there could be an amicable arrangement (only?) if the complaint is valid. In the Portuguese DPA annual reports, complaints related to a variety of issues (not only GDPR, but also LED) are counted together.[226] The Hellenic DPA reported in 2018 a high increase in the conclusion of complaints, apparently coinciding with the counting as 'concluded complaints' of cases where there was no longer a cause for action.[227]

The main takeaway is thus that national reporting practices appear to **reflect and sustain inconsistencies in national practices for the handling of complaints**, as well as the recurrent lack of clarity as to what can be expected after lodging a complaint with a DPA.

3. Findings of empirical research regarding DPAs' handling of complaints

To shed further light on existing practices concerning the facilitation of complaints submission by DPAs, we conducted empirical research based on the observation of a set of selected DPAs websites,[228] and reviewed publicly available information on one-stop-shop decisions.

3.1. Observation of DPAs websites

The main objective of the exploration of DPAs websites was to assess compliance with Article 57(2) of the GDPR, and thus to examine whether DPAs effectively facilitate the online submission of complaints, and how. As this assessment is concerned broadly with access to data protection remedies, including with Article 78 on the right to effective judicial remedy against a DPA, special attention is also given to the (or lack of) information made available to data subjects that may allow them to effectively exercise their right under Article 78 of the GDPR.

The examined websites are those of the Austrian DPA, Datenschutzbehörde (DSB);[229] Belgian DPA, Gegevensbeschermingsautoriteit (GBA);[230] the Berlin DPA, Berlin Commissioner for Data Protection and Freedom of Information (Berliner Beauftragte für Datenschutz und Informationsfreiheit, BlnBDI);[231] the Dutch DPA, Autoriteit

[224] See: GBA, *Jaarverslag 2018*, 2019 (the report has no page numbers); GBA *Jaarverslag 2019*, 2020, p. 67; and GBA, *Jaarverslag 2020*, 2021, p. 55.
[225] See e.g. AP, *Jaarverslag 2019*, p. 74.
[226] CNPD, *Relatório de atividades de 2019/2020*, 2021, p. 8, under '*Processos de natureza deliberativa'*.
[227] Ετήσια έκθεση 2018 (Annual report 2018), p. 33: *'..διεκπεραίωση καταγγελιών το έτος 2018 αυξήθηκε κατά περίπου 90%, με τη μεγάλη αύξηση να οφείλεται και στην αρχειοθέτηση αριθμού καταγγελιών λόγω απώλειας ενδιαφέροντος'*.
[228] On the importance of websites for DPAs, see: Kantor Management Consultants (2007), *Evaluation of the Means used by National Data Protection Supervisory Authorities in the promotion of personal Data Protection: Final report,* p. 17.
[229] https://www.dsb.gv.at.
[230] https://www.dataprotectionauthority.be.
[231] https://www.datenschutz-berlin.de/.

Persoonsgegevens (AP);[232] the French DPA, Commission Nationale de l'Informatique et des Libertés (CNIL);[233] the Hamburg DPA, Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI);[234] the Italian DPA, Garante per la Protezione dei Dati Personali;[235] Irish DPA, the Data Protection Commission (DPC);[236] the Lithuanian DPA, Valstybinė duomenų apsaugos inspekcija / State Data Protection Inspectorate (SDPI);[237] the Portuguese DPA,Comissão Nacional de Proteção de Dados (CNPD),[238] the Polish DPA, Urząd Ochrony Danych Osobowych;[239] the Spanish DPA, Agencia Española de Protección de Datos (AEPD).[240]

This research was carried out in April 2022. Changes might have been implemented since then. It is also important to note that when the researcher could not find a specific piece of information this does not necessarily mean that the information was absent from the website; it does indicate, however, that it was certainly not easily accessible, even for an individual attentively seeking it. Based on the research, a series of findings must be highlighted.

3.1.a. It is generally not difficult to find out how to lodge a complaint

All examined DPA websites offer a possibility to lodge complaints 'electronically', and generally speaking it is not difficult to find and access the relevant form in order to submit a complaint, once the data subject has reached the website of the DPA. From the homepage of the DPA website, submitting a complaint is most often only a few clicks away (typically between two and five, depending on the DPA and the exact path followed by the data subject).

Often, the possibility is visibly featured on the homepage of the DPA, even if sometimes a reference only becomes visible after scrolling down (e. g., Belgian DPA) or via a menu (e. g., Hamburg DPA). On the website of the Dutch DPA, the possibility to lodge a complaint is particularly prominent – a special button appears in the upper right corner of the page, in a contrasting colour.[241] Similarly, on the homepage of the CNIL there is a red button and a red logo, announcing a section called 'To act' or 'seeking help'; however reaching the relevant page to file a complaint will only happen after several click or after an interaction with an FAQ providing you additional information on the issue you are seeking to file a complaint about.[242] On the website of the Irish DPA, in contrast, it is not immediately obvious where a complaint can be lodged. A number of active steps are required from the data subject in order to reach the right destination.[243] On the Portuguese DPA website, there is the possibility to click on '*Apresentar queixa'*, which leads to a page on '*Participações*',[244] which appears to

[232] https://autoriteitpersoonsgegevens.nl.
[233] https://www.cnil.fr/.
[234] https://datenschutz-hamburg.de/.
[235] https://www.garanteprivacy.it.
[236] https://www.dataprotection.ie/.
[237] https://vdai.lrv.lt/.
[238] https://www.cnpd.pt.
[239] https://uodo.gov.pl/.
[240] https://www.aepd.es/es.
[241] Indicating '*Klacht melden'*.
[242] *'Agir : Comment faire valoir ses droits sur ses données ou agir en cas de problème ?*'.
[243] Navigate to the heading '*Your data'* and then to the sub-section '*Exercising your rights'*, then *'How can I complain to the DPC'*. Under this heading there is a button: '*Raise a concern with the Data Protection Commission'*.
[244] See: https://www.cnpd.pt/cidadaos/participacoes/.

be the right page for complaints under Article 77 of the GDPR even if the term used for complaints in the Portuguese version of the GDPR is another term ('*reclamações*').

Sometimes, the navigation path to reach the online complaint form is not straightforward, requiring some possibly not intuitive choices.[245] This presupposes that the data subject knows his rights in advance and that an online complaint form, or instructions on how to lodge a complaint, must be provided on the website of a DPA. In some instances, information about the right to lodge a complaint with the DPA can be found on the same page as the one with information about the rights of the data subject (e. g. Austrian DPA),[246] while in other cases it is on a different page. On the Spanish DPA website, there is a section with 'practical information', which refers to a series of pages, none of which relates to the lodging of complaints. Individuals are supposed to know they must click on a button named 'electronic office'.[247] Occasionally (e. g. Lithuanian DPA), it is much quicker to use the search function than to find the complaint form by scrolling down the home page of a DPA.

In some cases, the DPA puts forward different possibilities to individuals visiting the website, in case they would prefer for instance not to lodge a complaint but rather do something else. For example, when trying to submit a complaint to the Belgian DPA, the data subject will also find information about other options, notably about the possibility to submit a request for mediation, or a request for information. The Italian DPA gives the possibility to submit *'reclami'* (complaints) or *'segnalazioni'* ('tips'). Some DPAs appear to allow data subjects to lodge complaints only reluctantly, and even if they do make it possible for complaints to be lodged, they certainly do not appear to favour or actively promote this action (e. g. Irish DPA).

When considering submitting a complaint with the Dutch DPA, the data subject will find information about the possibility to submit a 'tip'.[248] Such tips may be submitted anonymously, and do not necessarily have to concern the processing of personal data of the person submitting the tip. The Dutch DPA explicitly warns visitors of the fact that although it uses tips to make research and policy choices, tips do not lead to an individual investigation, and the person submitting the tip will not receive a substantive response from the authority.[249] *A contrario sensu*, this might lead the visitor to expect a substantive response if they go through the complaint submission procedure.

In some cases, data subjects are invited to first consider contacting other actors. The website of the Belgian DPA indicates that if the issue at stake concerns a complaint about a theme also falling under the competence of another governmental service, the data subject can also approach the other service, and an example is given referring to unsolicited e-mails and

[245] On the Hamburg DPA website, the "complaint form for citizens" (DE: Beschwerdeformulier für Bürgerinnen und Bürger) is to be found in the menu "services/ media literacy" (DE: Services/ Medienbildung). On the Lithuanian DPA website, the complaint form is available under the menu for 'handling the complaints', individuals have to infer that a right to lodge or lodge a complaint can be exercised by pressing this link.
[246] See: https://www.dsb.gv.at/aufgaben-taetigkeiten/rechte-der-betroffenen.html.
[247] '*Sede electrónica'*.
[248] Concretely: '*de AP informeert (tip geven)'*.
[249] '*Een klacht melden waarbij u de AP informeert (tip geven): Vermoedt u dat een organisatie persoonsgegevens verwerkt op een manier die in strijd is met de privacywet? Dan kunt u de AP hierover informeren. U geeft dan een tip aan de AP. Een tip kan gaan over uw eigen persoonsgegevens, maar ook over persoonsgegevens van andere mensen. Of over de naleving van de privacywetgeving door organisaties in het algemeen. U kunt een tip anoniem indienen. De AP gebruikt tips om onderzoeks- en beleidskeuzes maken. Uw tip leidt niet tot een individueel onderzoek. Ook krijgt u geen inhoudelijke reactie van de AP*', https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/gebruik-uw-privacyrechten/klacht-melden-bij-de-ap.

unsolicited telephone calls.[250] The Lithuanian DPA encourages data subjects to check a list of public authorities dealing with data protection issues in order to make sure that they lodge a complaint with the right institution.[251]

Some DPA websites were perceived as offering much information about complaints, but scattered around sections and documents (e. g. NL), and not in a very clear and transparent manner (e. g. BE). The Lithuanian DPA encourages data subjects to become acquainted with three different sources, a page with general information and an invitation to first contact the DPA,[252] another about complaints concerning direct marketing,[253] and a specific document about common reasons leading to the inadmissibility of complaints.[254]

3.1.b. DPAs use different technical approaches for the submission of complaints

The obligation mentioned in Article 57(2) of the GDPR, according to which *'a complaint submission form which can also be completed electronically'* must be available, has mainly been translated into two main types of solutions. Some DPAs invite data subjects to complete online forms – to be filled in directly on the website -, while others give the possibility to download and complete a document, later to be sent to the DPA.

The Belgian DPA, for instance, makes available a form that can, once completed, be either uploaded to the website, or sent by mail.[255] This is also the case with the Italian DPA.[256]

Some DPAs rely on the submission of complaints on pre-existing national public portals. This is arguably a problem to the extent that it does not necessarily facilitate the lodging of complaints online, as generic forms might not be adapted for the needs of GDPR complaints.

To lodge a complaint with the Polish DPA, it is possible to send a letter, or do it orally at the seat of the Office, but if the data subject wishes to lodge a complaint online, they must do it via the 'ePUAP2' portal (the Polish digital government system).[257] The 'ePUAP2' portal requires that usage of an online form named 'General letter to a public body', which is a generic form, not specifically designed for GDPR purposes.

---

[250] https://www.gegevensbeschermingsautoriteit.be/burger/acties/klacht-indienen.

[251] 'DUK. Kokios institucijos Lietuvoje sprendžia asmens duomenų ir privatumo apsaugos problemas?' (https://vdai.lrv.lt/uploads/vdai/documents/files/08%20Duomenu%20apsaugos%20institucijos%202019-06-21.pdf). For example, the Lithuanian DPA suggests contacting the Office of the Inspector of Journalist Ethics in case of concerns of publishing personal data on social media platforms, or law enforcement authorities in case of an identity theft.

[252] 'Atmintinė asmenims, ketinantiems kreiptis į Valstybinę duomenų apsaugos inspekciją dėl skundo pateikimo', https://vdai.lrv.lt/atmintine-asmenims-ketinantiems-kreiptis-i-valstybine-duomenu-apsaugos-inspekcija-del-skundo-pateikimo.

[253] Atmintinė abonentams ir registruotiems elektroninių ryšių paslaugų naudotojams dėl informacijos pateikimo nagrinėjant skundą, susijusį su elektroninių ryšių paslaugų naudojimu tiesioginės rinkodaros tikslu, https://vdai.lrv.lt/atmintine-del-informacijos-pateikimo-nagrinejant-skunda-susijusi-su-elektroniniu-rysiu-paslaugu-naudojimu-tiesiogines-rinkodaros-tikslu.

[254] Dažniausiai Pasitaikantys Atvejai, Kai Valstybinei Duomenų Apsaugos Inspekcijai Pateikti Skundai Pripažįstami Nepagrįstais, https://vdai.lrv.lt/uploads/vdai/documents/files/Atvejai_kai_skundai_nepagristais_2019-05-06.pdf.

[255] https://www.gegevensbeschermingsautoriteit.be/burger/acties/klacht-indienen.

[256] https://www.garanteprivacy.it/diritti/come-agire-per-tutelare-i-tuoi-dati-personali/reclamo.

[257] https://epuap.login.gov.pl.

Online forms specifically created for a DPA can be a single generic form, or a series of forms adapted to different scenarios. The possibility to use a form adapted to a concrete concern may be of help for data subjects. Nevertheless, it can also be that the proposed forms appear to not fully cover all the cases in which a data subject might wish to lodge a complaint. The Irish DPA submission process obliges data subjects to choose one of a set of pre-defined categories,[258] which do not include a catch-all category (such as '*I have another type of concern'*). Some possible concerns – such as, for instance, non-compliance with a principle of Article 5 of the GDPR principle - do not seem to fit within these pre-specified options.

In a similar vein, the Austrian DPA gives the possibility to choose between different forms to lodge complaint,[259] but it is not clear how these forms would cover all possible scenarios in which a data subject might wish to lodge a GDPR complaint.

Sometimes, online forms appear to attempt to nudge data subjects into certain practices, possibly with the intention of reducing the number of lodged complaints that will have to be declared inadmissible, but generating some legal problems and affecting their right to lodge a complaint. A Spanish DPA template for complaints on the exercise of rights, for instance, cannot be submitted if the date indicated as the date of the exercise of the right is not, at least, a month ago (if that it is not the case, an error message appears). This can make sense if the complaint is about a lack of reply, as the data subject should wait one month. It does not seem appropriate, however, if the complaint concerns a received reply, the content of which was unsatisfactory; because of the design of the template, the data subject is being obliged to wait until a month has elapsed, without a proper legal justification.

Completing an online template is rarely the only available option, although it appears to be the only option on the Portuguese DPA website.[260,]
Submitting a complaint online appears now in any case as the main default option for many DPAs, even if other options are available.

To lodge a complaint with the Hamburg DPA, data subjects may also send a complaint by post or encrypted email, which could be a preferred option in case of submission that contains special categories of personal data as defined in Article 9 of the GDPR.[261] In case of questions about the electronic complaint or when a data subject prefers another form of contact, he/she can contact the Hamburg DPA by any other means (linking to a website with contact details, e.g. phone numbers, email address and PGP public key).[262]

With the Irish DPA, online complaint submission is presented as the primary submission mechanism, with alternatives only available to those who have specific accessibility requirements.[263] These individuals can contact the accessibility officer (for this, a postal and e-mail address is provided, although no phone number).

---

[258] Such as: '*I believe an organisation holds incorrect personal data about me and I wish to have it corrected', 'I want an organisation to delete personal data that it holds about me'*, '*I want to restrict the use of my personal data by an organisation'*, '*I want to object to the use of my personal data by an organisation'*, '*I want to delist search engine results relating to me (the "right to be forgotten")*'. The exact categories put forward appear to change depending on the path followed by the data subject.
[259] https://www.dsb.gv.at/download-links/dokumente.html.
[260] https://www.cnpd.pt/cidadaos/participacoes/.
[261] See: https://datenschutz-hamburg.de/beschwerde/.
[262] See; https://datenschutz-hamburg.de/pages/dienststelle/.
[263] Accessibility issues are defined quite narrowly in relation to the Disability Act (and so might not include issues around technological awareness, for instance).

Most often DPAs do not foresee special help communication channels to help data subjects during the submission of a complaint. There might be references to pages or documents with additional information. Otherwise, data subjects can generally search for the general contact information. Typically, most DPAs provide for the possibility to be reached by phone, or accept questions by email. In the contact section of the Irish DPA, it is noted that the most efficient and effective way to deal with the DPC about queries and complaints is the webform.

3.1.c. DPAs have variable requirements regarding supporting evidence or prior actions related to a complaint

Depending on the DPA, and sometimes depending on the form of submission, there might be different requirements in terms of supporting evidence.

When submitting an online complaint to the Polish DPA, it is presented as necessary to provide evidence confirming the circumstances (e.g., correspondence with the controller, contracts, certificates) as an attachment, as well as an electronic signature. Technically it is nevertheless possible to 'submit' without attachments – the DPA will then reach out to the data subject with a request to submit missing documents within a specified deadline.

The Hamburg DPA presents the possibility to attach files as an option, not an obligation, noting the data subject might send files that clarify the facts of the complaint, e.g. screenshots or scanned letters.[264]

There seems to be a divide among DPAs regarding complaints requirements and whether it is necessary to document a prior correspondence with the data controller also in cases unrelated to the exercise of data subject rights. Overall, DPAs recommend and encourage data subjects to first resolve any data protection issue by bringing it to the attention of the data controller (e. g. Lithuanian DPA and Hamburg DPA). The Hamburg DPA, for instance, clearly frames contacting first the data controller as a recommendation: it explains that often a data protection officer is available, and that the DPA receives a high number of complaints which could make contacting the data protection officer of the responsible body a quicker way to take action.[265]

Sometimes requirements are not presented as imperative conditions as such, but implied in instructions given to data subjects (e.g. in the complaint form). The Irish DPA, for instance, seems to hint that data subjects must have first contacted an organisation about their concern, and can only proceed to lodge a complaint with the DPA if they are not satisfied with the outcome.[266] Sometimes there is a fine line between advice and instruction; for instance, the French DPA invites data subjects to first contact the relevant organisation, without indicating if this would be compulsory.[267] When a complaint is being submitted, the French DPA insists

[264] See: https://datenschutz-hamburg.de/beschwerde/.
[265] Idem.
[266] Cf. '*if you have contacted an organisation about a personal data concern, in keeping with the guidance provided in our 'Know Your Rights' section and you are unhappy with the outcome, you can raise the matter with the Data Protection Commission through our online form'*. In the form, the data subject is only able to proceed if they indicate that they have already contacted the data controller.
[267] See: https://www.cnil.fr/fr/adresser-une-plainte, under « *Un organisme public ou privé ne respecte pas les règles de protection des données ? ».*

that the controller should have been contacted, and in case of unsatisfactory answer contacted again, and that a complaint should be submitted only in case of persistent problem.[268]

Some DPAs appear however to impose on the data subject preliminary actions or evidence requirements that do not directly derive from the GDPR, and which might be in tension with the DPAs' obligation to facilitate the submission of complaints.

The online form of the Dutch DPA only allows for the submission of a complaint if a proof of communication with the organisation about which the complaint is about is also submitted. It is not possible to file a complaint if you have not contacted the organisation first. The DPA explicitly indicates that it will not consider a complaint if the submission fails to include evidence of correspondence with the relevant organisation.[269]

3.1.d. It is much more difficult to lodge cross-border complaints than national complaints

Submitting an online complaint from a Member State different from the Member State of the habitual residence of the data subject can be particularly difficult, if not sometimes impossible.

Special challenges are connected to the reliance by DPAs on 'e-government' portals. Some illustrative examples are provided below.

There are several ways to lodge a complaint against a data controller with the Lithuanian DPA.[270] Data subjects can use the Lithuanian e-government portal, or an e-delivery system that requires connection via the e-government portal. In addition, they can send documents via email signed with a qualified electronic signature or via registered mail. Alternatively, data subjects can deliver the complaint on-site.[271] The e-government portal can be accessed by logging in with an identity card (ID) and a card reader, or by using mobile signature and via online banking. . Afterwards, the complaint form requires the provision of an address, which in the online form must be an address in Lithuania.[272]

Electronic complaints with the Polish DPA may only be lodged via the ePUAP2 portal, which operates only in Polish. It is necessary to open an account, available only for those who have a Polish Social Security Number (PESEL) or ePUAP profile, or can confirm their identity online. The identity can be confirmed either by a paid qualified certificate or by a free 'trusted profile'. The 'trusted profile' can be established only via logging into Polish electronic banking services or via a visit to a municipality. Non-residents usually will not have PESEL or a Polish bank account, so verifying the profile may be challenging. Although there is an option 'Use eID of your country' on the website that allows you to choose access from other EU Member States, the link was not working at the time this research was conducted.

---

[268] Which is not, as such, a GDPR requirement.
[269] In case the complaint concerns a state authority or other governing body ('bestuursorgaan'), the data subject is required to first formally object to their decision or file a lawsuit with the administrative judiciary.
[270] https://vdai.lrv.lt/lt/veiklos-sritys-1/skundu-nagrinejimas. See sections 'Skundo pateikimas elektroniniu būdu' and 'Galimi kiti dokumentų pateikimo būdai'.
[271] Idem.
[272] https://www.epaslaugos.lt/portal/service/101221/2020.

Electronic complaints with the Spanish DPA can only be lodged through an 'electronic office' requiring that the data subject follows a series of instructions for identification.[273] Eventually, if attempting to login from another Member State, the data subject will be sent to a 'Cl@ve' page in which appears a special button for EU citizens, which leads to a European authentication with foreign eID page,[274] which when used by Belgian residents leads to the Belgian service 'itsme'. An attempt to connect via 'itsme', despite successful identification, eventually led to a page indicating '*Something went wrong',* and referring to a general help desk. It appeared thus impossible to lodge a complaint online from Belgium – and the only alternative offered is to download a template, print it out, sign it, and send it following strict requirements (within the following 15 days).

In some cases, DPAs are making efforts so data subjects can lodge complaints online from other Member States.

This is the case for instance of the Hellenic DPA. After reaching the relevant page,[275] it is apparent there are primarily two ways for submitting a complaint. The regular way is online, by connecting to the authority's e-services portal through the citizen's 'taxisnet' credentials (user authentication credentials which allow access to the Hellenic state tax authorities and other e-government services). If accessing the authority's e-services is not possible, then the authority provides exceptionally other ways. The English version of the webpage explains that if logging in to the online portal using the 'taxisnet' credentials is not possible (because the complainant does not reside or work in Greece, or the representative body does not have an establishment in Greece) but Greece is the place of the alleged infringement, the DPA will accept the submission of complaints in English via e-mail.

The Hellenic DPA stands out positively in relation to the information it provides about all the possibilities foreseen under Article 77 of the GDPR. It devotes a specific tab to the question of 'Who can submit a complaint?',[276] and the answer suggests that it is possible for data subjects to submit a complaint, if Greece is their habitual residence or place of work, or the place of the alleged infringement.[277]

In relation to identification requirements imposed through the use of e-governmental portals, it must be highlighted that the GDPR does not in itself impose any particular identification requirements, and thus those appear to derive either from national laws, or through the technical choice of requiring access to a portal that imposes strict identification. The threshold for identification is otherwise very low in some settings, with DPAs for instance accepting emails with no specific identification proof.

Sometimes, the difficulties to lodge a complaint from another Member State emerge when completing the complaints form. When lodging a complaint with the Dutch DPA, the data

---

[273] '*Para realizar la firma con su certificado digital es preciso que tenga instalada en su equipo la aplicación Autofirm@ del Ministerio de Hacienda y Función Pública. ¿La tiene ya instalada? Pulse 'Aceptar' en caso afirmativo o si va a elegir autenticarse con Cl@vePIN o Cl@ve Permanente'.*

[274] https://eidas.redsara.es/SpecificConnector/CountrySelector.

[275] In Greek, https://www.dpa.gr/index.php/el/polites/katagelia_stin_arxi, and in English, https://www.dpa.gr/en/individuals/complaint-to-the-hellenic-dpa.

[276] In Greek, you can refer to the section: 'ποιος μπορεί να υποβάλει καταγγελία'.

[277] The same section also adds: '*Data subjects have the right to assign non-profit bodies or organizations or unions or associations that legally operate, have statutory goals of general interest and operate in the field of protection of rights and freedoms of data subjects with regard to data protection, to submit a complaint, to the Hellenic DPA, on their behalf'.*

subject must fill in the place of residency. If one indicates a zip code that does not adhere to the Dutch formula (4 numbers, 2 letters) the form does not accept it. It is unclear whether filling in a random but existing Dutch zip code will result in the Dutch DPA declaring your complaint invalid.

The online template used by the Irish DPA includes a pre-registered reference to an Irish phone prefix, and a reference to an Irish postcode. These can be ignored, but doing so requires that the data subject is aware of the fact that it is legally possible to submit a complaint while not residing in Ireland, and has enough confidence in their knowledge to still complete the form and submit the complaint.

Language might often be an obstacle for some data subjects to lodge a complaint with a DPA different than the one of the Member State in which they reside or work. Numerous DPAs do offer some information in other, non-national languages – mostly in English (e. g. Poland, Belgium). The website of the Portuguese DPA seems to be designed to be available both in Portuguese and in English, although the English version is under construction.[278]

Even in cases in which the website offers some information in English, it might be that the information about complaints is not available in English (e.g., Italy) or it is not possible to lodge complaints in a language different from one of the national languages (e.g. Poland, Lithuania, and Belgium)[279]. The Austrian DPA is clear about the fact that complaints must be in German.[280] Sometimes language requirements are not completely clear by visiting the website. With the Hellenic DPA it does seem possible to lodge complaints in English.

The website of the Dutch DPA can be visited in Dutch and in English. When switching to the English version, however, the already mentioned 'lodge a complaint' contrasting button disappears.[281] Moreover, most of the dropdown menu options disappear as well. When searching for 'complaint' on the English version of the website, no results for 'lodge a complaint' come up. It therefore appears it is only possible to file a complaint on the Dutch version of the website. According to the online Q&A and the form itself, it is possible to lodge a complaint via (physical) mail, the digital form on the DPA website and via the phone. The authority does mention that it is possible to lodge a complaint in English as well, but this is not facilitated via the online complaint form. It seems as if it is only possible via mail and telephone, but again, this information is not available on the English version of the website, only on the Dutch version. The online form is only available in Dutch.[282]

---

[278] This message is displayed: '*Work in progress! The Portuguese data protection authority is remodeling its website. Please feel free to visit us again soon*!', https://www.cnpd.pt/en/.

[279] When navigating the English version of the Belgian DPA website, it is not possible to submit a complaint: the data subject is referred to other linguistic versions. This is consistent with Art. 60 of the Law of 3 December 2017 on the creation of the Data Protection Authority, which conditions the admissibility of complaints to the use of one of the national languages.

[280] The AT annual report of 2018 even reveals that English complaints will be rejected by the Austrian DPA due to formal reasons, as it is embedded in the law that all complaints must be in German (see also https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20180921_DSB_D130_092_0002_DSB_2018_00/DSBT_20180921_DSB_D130_092_0002_DSB_2018_00.html). See: Datenschutzbehörde (DSB), *Datenschutzbericht 2018,* 2019, p. 16 and pp. 23-24.

[281] See: https://autoriteitpersoonsgegevens.nl/en.

[282] https://autoriteitpersoonsgegevens.nl/nl/meldingsformulier-klachten. According to the EDPB document *Handling cross border complaints against public bodies or authorities*, pursuant to Dutch administrative law (Article 2:6 of the General Administrative Law Act, GALA), languages other than Dutch may be used, but only if and where this use is more effective and does not disproportionately disadvantaged the interests of third parties; the Dutch DPA noted that '[o]ther than English, no language would satisfy these criteria, especially the

Similarly, the French DPA offers an English version of its site on which it is unclear if and where to find the complaint form available on the French version. When typing 'complaint' in the site search function, information about cases and complaints dealt with by the CNIL will appear but no obvious link or information on how to file a complaint.

3.1.e. DPAs provide heterogenous proofs of submission

For the data subject to eventually be in a position to exercise their right to an effective judicial remedy under Article 78(2) of the GDPR, they must have proof of the fact they submitted a complaint, and when. Yet, the way in which DPA's (fail to) provide such proof, differs widely.

The Irish DPA informs data subjects about the fact that it will not acknowledge electronically the submission of complaints. Data subjects are asked to download a copy of the complaint submitted, should they wish to retain it for their records. When lodging with the Berlin DPA, the data subject sees a thank you message.[283] They are instructed to print the form before submitting if they wish a copy, and there will be no email acknowledgement of receipt.

When a complaint is lodged with the Hamburg DPA, the data subject receives a summary of the entry as a PDF that downloads automatically; in addition, the website itself acknowledges receipt together, with a reference number and a telephone contact number.[284]

After submitting with the Lithuanian DPA, it is possible to download and print its copy, including a time stamp and all information provided; however, no email confirmation is sent. When lodging a complaint with the Portuguese DPA, the individual will receive proof of submission by e-mail only if they actively chose that option.

The Dutch DPA sends a confirmation email (from a 'no-reply' email address) which is however not a copy of the complaint, and does not contain the date of submission as such. A similar confirmation email is sent by the Austrian DPA. The French DPA also sends an acknowledgment of receipt, with a reference number. It is not possible to reply to that email, but the complainant is encouraged to contact the DPA for any inquiries or remarks by phone, fax or mail.

3.1.f. Data subjects received limited information on next steps after lodging a complaint

For the data subject to eventually be in a position to exercise their right to an effective judicial remedy under Article 78(2) of the GDPR, they must also have information about the existence of their right.[285] If they are not aware of the fact that they can launch proceedings against the DPA if not informed within three months on the progress or outcome of the complaint, there is little chance they will exercise their right. Most DPAs, however, **fail to inform complainants about Article 78(2) of the GDPR** after the submission of a complaint.

---

criterion of effectiveness', so it would be able to accept complaints if they are in either English or Dutch (at least against public bodies or authorities, p. 8).

[283] '*Vielen Dank für die Übermittlung des Beschwerdeformulars'*.

[284] The text reads like this: '*Thank you for your complaint. We have received your complaint. If you have any queries, please contact us by email or telephone (...) quoting reference number (...)'*.

[285] It is the task of DPAs to generally promote awareness of data protection rights (Art. 57(1)(b) GDPR).

After submitting an online complaint with the Irish DPA, the data subject is provided a text to the effect that if the complaint has merit it will be followed up in 20 working days, although the language is quite vague ('*we will endeavour to progress your complaint'*).[286]

An example of best practice can be found with the Italian DPA which mentions that there is a right to effective judicial remedy against the DPA, explicitly mentioning Art. 78 GDPR.[287] The Austrian DPA refers to the fact that it has to give an initial response within three months and issue a final decision within six.[288]However, it does not inform the data subject about the fact that if the authority fails to react within three months it might be possible to take action under Article 78(2) of the GDPR.

On the website of the Polish DPA, general information on what to expect next is limited and vague. The data subject is informed that submitting a complaint shall initiate administrative proceedings conducted by the DPA in accordance with the procedure, principles and deadlines provided for by law.[289] After lodging a complaint with the Belgian DPA, the data subject is informed that the complaint will be handled by the relevant department to provide a substantive answer as soon as possible. After submitting to the Portuguese DPA, the data subject is told that the authority 'will proceed accordingly'.

After submitting with the Lithuanian DPA, the data subject is referred to a seven page document,[290] according to which the complaint shall be 'addressed' within three days.

The Dutch DPA does refer to the three month period, as the page visible after the submission of the complaint indicates that a progress report will be sent within three months. In the Q&A section of the complaint page the DPA elaborates on this by answering the question 'When will I get a reaction on my complaint?': it states it will respond within three months, and if there are no results to report after three months, it will contact the data subject again six months later. The Berlin DPA, in its 'information sheet' (*Merkblatt*)[291,] also refers to the fact that the DPA will inform the complainant of the (interim) result of its review within three months of receiving the complaint.

The email automatically sent by the French DPA after the submission of a complaint states that a decision will be taken on the admissibility of the complaint within a month, and the complainant will be informed about the outcome of such decision by mail ('*par courrier'*). The French DPA's website states that the authority will do its best to keep the complainant informed, and that the time required to handle the complaint might be affected by factors such as the total number of complaints received or the wait for a judgment, such as a

---

[286] The text is: '*Please note that where you have included copies of relevant documents - your original request, or, where applicable, any evidence that shows a contravention of data protection legislation has occurred, and any response received from the organisation (data controller) - we will endeavour to progress your complaint within 20 working days'.*

[287] Available at a section about general information on 'how to protect your personal data', under section *'Strumenti di tutela - Il reclamo'*:
https://www.garanteprivacy.it/home/diritti/come-agire-per-tutelare-i-tuoi-dati-personali.

[288]See https://www.dsb.gv.at/aufgaben-taetigkeiten/rechte-der-betroffenen.html.

[289] https://uodo.gov.pl/pl/83/156.

[290] Order of the Director of the State Data Protection Inspectorate No 1T-20 (1.12.E) of 2 March 2021 'On the Approval of the Description of the Complaints Handling Procedure of the State Data Protection Inspectorate', Valstybinės duomenų apsaugos inspekcijos direktoriaus 2021 m. kovo 2 d. įsakymas Nr. 1T-20 (1.12.E) 'Dėl Valstybinės duomenų apsaugos inspekcijos nagrinėjamų skundų nagrinėjimo tvarkos aprašo patvirtinimo'.

[291] https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/beschwerde/BlnBDI_Merkblatt_Rechte.pdf.

judgment of the EU Court of Justice.[292] Although it does provide to the general public information on available judicial remedies against its decisions, it does not mention in the general information page about complaints anything about the remedy against inactivity. The French DPA in any case asks the complainant to wait at least two months before contacting the authority to ask about the status of the complaint.

Generally, limited information on the rights of the data subject – and more broadly about what can be expected in practice - is actively provided to complainants after lodging a complaint.

Beyond the information about deadlines, it would be useful for the data subject to know in advance that they can expect the DPA to adopt a legally binding decision as a final outcome of the complaint procedure. That is not always necessarily clear. The Irish DPA, for instance, stresses that its preference will be to seek an '*amicable resolution within a reasonable timeframe'*, noting it is mandated '*to facilitate or arrange an amicable resolution of the matter, where there is a reasonable likelihood of this being achieved, within a reasonable time'*.[293] According to the DPA, when amicable resolution is not possible, other outcomes might be for instance the rejection of the complaint, the dismissal of the complaint; or providing advice in relation to the matter, among others.

3.1.g. Data subjects get very limited information about the one-stop-shop

Most often, DPA websites do not inform data subjects who are about to lodge a complaint about the possibility that the complaint will have to be handled under rules applying for some cross-border processing cases (that is, under the **one-stop-shop**). In practice, this means that data subjects often are not made aware that another DPA may end up leading on the case related to their complaints.

Although there are sometimes references to potential information sharing through the Internal Market Information System (IMI), it is often not made clear that a decision might end up being adopted through Article 60 of the GDPR: it is for instance not clear when lodging a complaint with the Portuguese DPA, or with the Belgian DPA.

Sometimes, there is online information about the one-stop-shop, but it is not made available specifically before or while lodging a complaint. The Dutch DPA, for instance, explains the one-stop-shop on a different page.[294] Otherwise, the authority does mention that if the data subject filed a complaint 'about an international organisation', the Dutch DPA may have to handle it together with other DPAs, slowing down the procedure.[295]

The Austrian DPA mentions that if the controller against whom the complaint is directed is located outside of Austria, the procedure might be transferred to another DPA. There is however no step-by-step explanation of the whole procedure.

---

[292] See: https://www.cnil.fr/fr/adresser-une-plainte, under « *Après l'envoi de votre plainte* ».
[293] See: https://www.dataprotection.ie/en/individuals/exercising-your-rights/complaints-handling-investigations-and-enforcement-individuals.
[294] See: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/een-loketmechanisme-one stopshop.
[295] See: https://autoriteitpersoonsgegevens.nl/nl/behandeling-van-klachten-door-de-ap.

3.1.h. Very limited information is provided on NGOs that might help lodge complaints

Generally, it is technically possible to lodge complaints online not just for data subjects, but also for other individuals or not-for-profit bodies, organisations or associations representing them. This possibility might sometimes only become visible as the relevant submission form is being completed (e. g. Irish DPA).[296] Sometimes, what becomes visible is the possibility to represent somebody else based on the power of attorney (e. g., Hamburg DPA).

Nevertheless, data subjects visiting DPA websites to lodge a complaint, or seeking more information about the procedure, will generally not encounter any information about their rights under Article 80(1) of the GDPR.

On the website of the Dutch DPA, there is information about the possibility of mandating in the Q&A complaints section under 'Who can lodge a complaint?': the authority says that a data subject can proxy/authorise someone to lodge a complaint for them, e.g. a lawyer, a legal helpdesk ('*Juridisch Loket'*) or a civil rights organisation/NGO ('*belangenorganisatie*').

The Hellenic DPA offers particularly detailed information about this, noting '[d]*ata subjects have the right to assign non-profit bodies or organizations or unions or associations that legally operate, have statutory goals of general interest and operate in the field of protection of rights and freedoms of data subjects with regard to data protection, to submit a complaint, to the Hellenic DPA, on their behalf'*, and offering information about the steps to submit a complaint as an association.[297]

3.2. Observation of the EDPB Register of Article 60 decisions

The EDPB makes available through its website a collection of what it calls 'final decisions' adopted under the one-stop-shop.[298] This Register is made publicly available by the EDPB despite the lack of any explicit legal obligation to do so. The Register does not claim to be exhaustive, and is notably accompanied by a series of disclaimers pointing out that some decisions will not published in the register, or will be published in a partially redacted way, *'(d)ue to national legal restrictions'*, without specifying nevertheless the exact legal basis of the restrictions. The Register is also not systematically updated, but updated irregularly, at unpredictable intervals. Despite its limitations, the Register constitutes an extremely valuable resource for researchers and interested stakeholders to explore the functioning of the one-stop-shop in practice.

In connection with the object of this study, what is most important to underline is that the documents available reveal **a number of apparently inconsistent ways of applying the**

---

[296] These choices are presented at a certain point: '*You are:' 'Acting on behalf of a relative without the capacity to do so themselves*', '*A not-for-profit body, organisation or association representing an individual'*, *'A not-for-profit body, organisation or association representing a number of individuals'*.

[297] Source: in Greek https://www.dpa.gr/el/polites/katagelia_stin_arxi, and more limited information in English https://www.dpa.gr/en/individuals/complaint-to-the-hellenic-dpa. It is worthwhile noting that the word 'ένωση' in the Greek version, is translated with both terms in the English version as quoted in the text above: 'union or association' (cf. Art. 80 GDPR, which does not refer to unions).

[298] Accessible here: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_el. The name of the URL is unfortunate, as actually the decisions presented are not 'consistency findings'.

GDPR, and especially a problematic lack of clarity as to what constitutes the outcome of a complaint, both at the level of DPAs and at the level of the EDPB.

In this sense, it can be noted that the Register divides decisions based on the case 'outcome' by grouping them under these labels: reprimand, no violation, no sanction, compliance order, dismissal of the case, administrative fine, and erasure order. Presumably, some of these 'outcomes' would clearly correspond to what the GDPR describes as dismissal or rejection of a complaint, and others to what constitutes to 'act on' the controller, but some such as 'no sanction' or 'no violation' do not necessarily fit clearly in a type of outcome, as it could be that there was 'no sanction' but there was a GDPR infringement.

The relations between all these outcomes are not always clear, as is often unclear how decisions are in line with Article 60 of the GDPR and EDPB guidance thereof.

In a decision dated from January 2022, for instance, the Cyprus DPA issued a reprimand as lead DPA related to a complaint that had been lodged in Germany, despite the fact that in the meantime the complaint had been withdrawn.[299] The case concerned an access request, and the data subject had eventually received the requested data. For the Cyprus DPA, the withdrawal of the complaint represented a mere mitigating factor. As there had been an infringement, concretely in the form of lack of timely reaction to the request, a reprimand was issued. It is unclear why this should not be treated as a '*demonstrated removal of the cause of action'* that, according to the EDPB, would justify the dismissal of the complaint – and thus be a decision to be adopted by the DPA that had received it. This decision is classified as 'reprimand', which seems logical and corresponds to a GDPR provision (Article 58(2)(b)).

The same DPA, in another decision also of January 2022, had to decide as lead DPA in a case about a complaint originating in Germany about the right to erasure.[300] An email was sent to the data controller, which explained it had deleted the data subject's data, and then the Cyprus DPA took the view that there had been only '*a minor infringement, which only slightly affects the data subject's rights and freedoms*'. Taking into account this and the data controller's cooperation, it '*considered the investigation proceedings concluded'*. There is no reference to the data subject possibly having withdrawn their complaint, and no real action appears to have been taken by the DPA beyond the sending of questions by email. It is unclear why this does not represent a rejection or dismissal of the complaint, a decision which should have been made by the DPA which received the complaint. The EDPB register does not classify this decision as such, but simply indicates 'no sanction'.

A decision from October 2021, adopted by the Luxembourg DPA, concerns a complaint that had been lodged with the DPA of Rhineland-Palatinate.[301] The controller, which had its main establishment in Luxembourg, had failed to reply to an access request by the complainant about the source of some payment data. The Luxembourg DPA contacted the controller, which gave details on where the data came from. After that, the Luxembourg DPA declared that it could not identify any infringement of the GDPR, and suggested to the DPA of Rhineland-Palatinate to 'close' the complaint, as no infringement had been identified. The Rhineland-Palatinate DPA agreed. The document published on the EDPB Register bears the

[299] See: https://edpb.europa.eu/decision-no-309_en.
[300] See: https://edpb.europa.eu/decision-no-316_en.
[301] See: https://edpb.europa.eu/decision-no-243_en. For a similar scenario, see: https://edpb.europa.eu/decision-no-242_en.

title ‘Final decision’, and is signed by the Luxembourg DPA, which can be interpreted as meaning that Article 60(7) of the GDPR was considered to be applicable, instead of Article 60(8), despite the fact that the decision could potentially be interpreted as a rejection or dismissal of the complaint. The Register describes the outcome as ‘no violation’.

A decision of September 2021, adopted by the Swedish DPA, is openly classified as having as outcome the ‘dismissal’ of the complaint – the final decision being to close the case without further investigation.[302] The case concerns, however, a complaint lodged with the DPA of the United Kingdom (UK). It is very unclear why Article 60(8) of the GDPR was not applied.

In May 2018, a data subject lodged a complaint with the Romanian DPA.[303] He complained that he kept receiving a newsletter despite multiple attempts to unsubscribe and a request to have his data deleted by the data controller. He accompanied the complaint with a number of screenshots, including of the newsletter received after the attempts to exercise his rights. In application of the one-stop-mechanism, the Hungarian DPA was identified as lead authority for this case. On 20 December 2018, the Hungarian DPA sent an email to the data subject, giving him eight days to provide some requested evidence and state information such as his full name, and his mother’s name and place and date of birth. Another email was sent after an undefined period. The language used in these emails is not known. In June 2020, in any case, the Hungarian DPA decided that the facts alleged by the data subject were not in any way substantiated or verified, and closed the case, ‘without an investigation of merit’, with a letter in English addressed to the data subject.[304] The EDPB Register classifies this outcome as a ‘dismissal of the case’. It is unclear why the decision to dismiss the case was not adopted by the DPA with which the complaint had been lodged.

Another case illustrating the position in which data subjects might find themselves relates to a complaint lodged in Germany on 25 May 2018.[305] The complaint, concerning Articles 5, 6 and 7 of the GDPR, was originally lodged with the Bonn DPA, and eventually reached the Brandenburg DPA. The Liechtenstein DPA was finally identified as lead supervisory authority. On 7 August 2018, the Liechtenstein DPA sent a letter to the data subject requesting additional information and evidence, giving them 14 days to reply. As no answer was received, an email was sent, demanding a reply for 30 August 2018. Taking into account the lack of answer, the Liechtenstein DPA decides to close the file, and eventually sends a letter to the Brandenburg DPA in this sense, dated 12 August 2019, indicating that, according to them, such decision might be appealed in front of the courts of Liechtenstein.[306]

4. Analysis

The research invites a series of reflections, taking into account the described legal framework and policy objectives, and the persistent challenges, as presented in the previous sections.

[302] See: https://edpb.europa.eu/decision-no-276_en.
[303] See: https://edpb.europa.eu/decision-nr-117_en.
[304] Available here: https://edpb.europa.eu/sites/default/files/article-60-final-decisions/pblsh_hu_2020-07_right_to_erasure_article17_dec.pdf.
[305] See: https://edpb.europa.eu/decision-nr-40_en.
[306] The letter also informs the recipient that the appeal period only starts after the court holidays period, which runs from 15 July and lasts up to and including 25 August of each year.

4.1. The facilitation of complaints submission should be improved

Facilitating the submission of complaints is not only a **legal obligation** for DPAs, but can also help them to **deal better with incoming submissions**. A clear and well-functioning system can reduce the problems found with some submissions, and generally reduce the need for data subjects to contact them to request assistance or further information.

Beyond this, there are some instances in which the absence of facilitation might actually undermine the rights of data subjects, most directly their rights under Article 77 of the GDPR.

An important issue is the **availability of information** about the possibility to lodge a complaint. DPA websites appear to assume that data subjects visiting them know in advance about the fact that they have a right to lodge a complaint. This might however not always be the case. Indeed, although data controllers are supposed to inform data subjects about the fact that they have the right to lodge a complaint with a DPA,[307] this does not always occur. Actually, it might be that precisely the concern of the data subject is an infringement of information obligations or a problematic response to an access request, and therefore it is even more likely that the information did not reach the data subject.

Once the data subject decides to lodge a complaint, the process is not always as smooth as desirable. Practical challenges emerge notably when DPAs, instead of complying with the letter of Article 57(2) of the GDPR - which obliges them to provide a complaint submission form which can be completed electronically - refer data subjects to generic forms on external platforms.

Whereas the EDPB announced in April 2022 it will '*propose a template for data subjects' complaints, to be used by DPAs on a voluntary basis'*, the objective of such initiative does not seem to be to facilitate the submission of complaints by data subjects as such, but rather **to facilitate cross-border exchange of information between DPAs**.[308] It is also in order to improve the efficiency of cooperation between DPAs that the EDPB referred in that statement to its intention to identify procedural aspects that could be further harmonised in EU law.[309]

4.2. Limited information is provided to complainants

Even if DPAs appear to be making efforts in informing data subjects before, and while they lodge complaints, little useful information is provided on what occurs next.

This lack of information is **problematic**, and it might constitute a disincentive to lodge a complaint. Reading Article 57(2) of the GDPR together with Articles 77 and 78, the obligation of facilitating the submission of complaints is not limited to simply technically facilitating the submission as such, but more broadly about facilitating the whole process. Therefore, it is essential that data subjects know how to lodge complaints, but also that they know the exact legal implications of the fact they have submitted a complaint.

[307] Art. 13(2)(d), 14(2)(e) and 15(1)(f) GDPR.
[308] EDPB, *Statement on enforcement cooperation*, adopted on 28 April 2022, p. 2.
[309] Idem.

At the latest immediately after data subjects have submitted a complaint, they should be provided information about the right under Article 78 of the GDPR – most crucially, about their right to effective judicial remedy in case they do not hear from the DPA after three months.

The increasing reliance on 'fast-tracking' procedures, implying a certain degree of informality and unpredictability, can also render it more difficult for data subjects to understand what is supposed to happen, and what they are entitled to demand from controllers and processors, and from DPAs.

Similarly, any procedures or avenues not resulting in public and/or contestable decisions may lead to less jurisprudence being developed and a loss of knowledge on how to interpret and apply the GDPR in a consistent manner.

Regarding information obligations imposed on DPAs, it must be recalled that Article 57(1)(f) of the GDPR makes an explicit reference to the need to '*inform the complainant of the progress and the outcome of the investigation within a reasonable period,* ***in particular if*** (...) ***coordination with another supervisory authority is necessary***'. This could be read as implying that when the one-stop-shop mechanism applies, appropriately informing the complainant is even more important than in domestic cases.

4.3. Significant opaqueness and fragmentation of complaint handling

The empirical research on DPA practices has shown discrepancies that concern very fundamental aspects of the submission and handling of complaints, with potentially serious implications on the level of data protection in the EU. The EDPB has emphasised that '*(d)ata subjects shall enjoy* ***equal access to exercise their right to data protection*** *regardless of which supervisory authority would handle a given complaint'*.[310] It is extremely doubtful if this is the case at this moment.

Recent trends towards handling with diverse degrees of intensity, coupled with the fact that DPAs websites often fail to provide useful information about the probable outcome of a complaint, make it difficult to exercise the Article 77 GDPR right in a meaningful way. The legal consequences of the different approaches being implemented at national level deserve **more scrutiny**. As an example of existing problem, the Belgian DPA warns prospective complainants that if their complaint is 'filed without follow-up' in line with the authority's own policy, policy which explicitly conditions the follow-up of complaints to the DPA's own priorities, the opposing party will be in principle informed, by receiving a copy of the decision filing the complaint. The opposing party will thus know, the DPA notes, that complaints on the subject matter at stake are not going to be further investigated.[311]

The will to seek 'friendly solutions' to data protection issues is not new, and many DPAs have made efforts in this direction for decades.[312] Currently it is primarily the responsibility of DPAs and of the EDPB to make sure the GDPR is enforced and applied consistently. It is however not clear that their actions will be enough.

---

[310] EDPB, *Internal Document 02/2021*, p. 4.
[311] APD – Chambre Contentieuse, Politique de classement sans suite de la Chambre Contentieuse, op. cit., p. 4.
[312] Cf., for instance, CNIL, *Dix ans d'informatique et libertés, Economica,* 1988, p. 72, referring to '*solutions amiables'*.

Despite the EDPB's activities in this realm during the last couple of years, **the fact is that the current state of complaints handling in the EU is still fragmented and opaque.** This is true both for standard, 'domestic', non-one-stop-shop complaints, and for complaints subjected to the one-stop-shop procedure, and has serious implications for the enjoyment of Article 77 of the GDPR (the data subject's right to lodge a complaint with a DPA) and Article 78 (the right to an effective judicial remedy against a DPA). As such, **it directly affects the EU fundamental rights to personal data protection (Article 8 of the Charter), and to an effective judicial remedy (Article 47 of the Charter)**.

As repeatedly illustrated above, the EDPB has been working on different aspects related to the lodging of complaints, and it has produced a number of documents useful to obtain a better understanding of the DPA approaches in this area.[313] For unclear reasons,[314] some of these documents have originally been adopted as EDPB internal documents, and not publicly shared. Nevertheless, some have in the meantime been rendered public through access to document requests by concerned individuals and civil society organisations. Sometimes the eventually disclosed EDPB documents refer to other documents in ways that make it difficult to know if they are referring to not-yet-disclosed documents.[315] The EDPB did eventually publish its *Guidelines 02/2022 on the application of Article 60 GDPR* but decided not to subject the document to a period of public consultation. The document that was to become the EDPB's *Guidelines 06/2022 on the practical implementation of amicable settlements* was originally adopted as Internal Document 06/2021, presumably because '*EDPB members decided to discuss the publication of the document after a period of 6 months, allowing the EDPB members to gain experience from practice during that time'*.[316] There was no public consultation on its content.

In light of the seriousness of the issues at stake, which directly concern EU fundamental rights, and the absence – in principle – of any particular interest to protect through secrecy, it is difficult to understand how this lack of openness can be justified. In any case, it appears to be unproductive and **contrary to the objective of ensuring a consistent application** of the GDPR.

Also, it is unclear which institution – if any – perceives itself as responsible for acting when DPA actions contradict (secret or non-secret) EDPB guidance. For example, as noted above, the EDPB has emphasised that DPAs should not require more than a substantiated complaint, presenting circumstances that explain the reason of the complaint – and data subjects should

---

[313] On 2 February 2021 the EDPB adopted its *Internal EDPB Document 02/2021 on SAs duties in relation to alleged GDPR infringements;* it emerges from its introduction text that in July 2019 the EDPB granted its Enforcement Expert Subgroup the mandate to, *inter alia, 'Develop a common interpretation of Article 57(1)(f) and a common understanding of the minimum requirements to fulfil the obligation to "investigate the complaint to the extent appropriate"* (p. 3).

[314] The EDPB Rules of Procedure establish as a general principle a principle of transparency: 'In accordance with the principle of transparency, the Board shall operate as openly as possible so as to be more effective and more accountable to the individual' (Art. 3).

[315] Cf. for instance the reference to 'Internal Guidance on Local Cases' in EDPB, *Internal Document 02/2021,* p. 13.

[316] EDPB, *Guidelines 06/2002 on the practical implementation of amicable settlements*, p. 2. There is no reference to such foreseen period for gaining experience in the original Internal Document (EDPB, *Internal EDPB Document 06/2021 on the practical implementation of amicable settlements*, adopted on 18 November 2021). The agenda of the meeting of the EDPB of 12 May 2022 did not foresee the adoption of the document in the form of standard Guidelines, but the publication of the Internal Document (cf. Agenda of 65th EDPB meeting, 12 May 2022 Remote). All accessible preparatory documents related to such Guidelines refer to them as Internal Guidelines (cf. request for access to documents 2022/27, submitted by Johnny Ryan to the EDPB).

be given the opportunity to elaborate on unsubstantiated issues before their complaint is dismissed. Despite this guidance, the research carried out shows that DPAs apply different requirements.

More broadly, it is important to note that a certain degree of uncertainty persists regarding some key aspects of cooperation between DPAs. Basic issues such as which national law applies when should be clear to all, including data subjects. Also, there is uncertainty on how the current approaches supported at EDPB-level (e. g. admissibility requirements determined by the Member State in which the complaint was lodged, procedural law applying to the investigation determined by the Member State of the lead supervisory authority, etc.) shall still to be considered in light of the exact relation between Article 77 and Article 79 of the GDPR,[317] on which there is also uncertainty pending clarification by the EU Court of Justice.

On this point, it must be noted that despite the wording of Article 77(1), according to which *'every data subject shall have the right to lodge a complaint*' with a DPA '*(w)ithout prejudice to any other administrative or judicial remedy',* several national laws establish that DPAs shall not handle complaints when the matter at stake is also in front of the courts.[318]

The EDPB has in the past highlighted that there exists a 'patchwork of national procedures and practices' related to *'differences in complaint handling procedures'*.[319] The EDPB noted in this regard that the European Commission should monitor national procedures, and that '*eventually legislators may also have a role to play in ensuring further harmonization'*.[320] While this might be correct to some extent, it is nevertheless also true that some differences in procedures emanate directly from DPA practices and DPA rules. In this sense, for instance, the Luxembourg DPA follows what it describes as 'internal rules of procedure' for the handling of complaints, adopted by the DPA itself, and made available through its website.[321]

4.4. Serious obstacles to the cross-border enjoyment of rights

Current practices by DPAs make it particularly difficult for data subjects not residing in a Member State to lodge a complaint with the DPA of such Member State. This is in direct tension with the most basic goals of the GDPR, based on the idea that everyone shall enjoy the same level of data protection '*whatever their nationality or residence'*.[322]

---

[317] Applicable law applying when courts adjudicate is itself also subject to debate; see, for instance: Ioannis Revolidis (2017), 'Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of"Privacy Tourism"?', *Masaryk University Journal of Law and Technology* 11(1), pp. 7-37.

[318] Ssee, for instance, the Lithuanian law obliging the DPA to reject the complaint if its subject matter – or part of it - has been examined or is being examined in the court of Lithuania or another Member State: EDPS/2019/02-07, February 2020, p. 3, and Milieu, *Study on the national administrative rules impacting the cooperation duties for the national supervisory authorities: Questionnaire for the national supervisory authorities (Lithuania),* EDPS/2019/02-07, February 2020, p. 4); see also, on the Slovak Republic, Milieu, *Study on the national administrative rules impacting the cooperation duties for the national supervisory authorities: Questionnaire for the national supervisory authorities (Slovak Republic)*, EDPS/2019/02-07, February 2020, p. 3. Further complicating the overall picture, the GDPR lacks specific rules for DPA coordination similar to those of its Art. 81, concerning the suspension of court proceedings in certain cases.

[319] EDPB, *Annual report 2019: Working together for stronger rights,* 2020, p. 10; EDPB, *Contribution of the EDPB to the evaluation of the GDPR under Article 97,* op. cit., p. 3.

[320] Idem.

[321] Commission nationale pour la protection des données (CNPD), *Procédure relative aux réclamations devant la CNPD,* https://cnpd.public.lu/dam-assets/reglements-cnpd/CNPD-Procedure-Reclamationsversdef20201016.pdf.

[322] Recital 2 GDPR.

Beyond the obligation to remove these obstacles, there could be an added-value in generally encouraging data subjects to consider lodging their complaints with the DPA of the place of infringement, if that would allow them to avoid the one-stop-shop and thus, possibly, obtain a better follow-up to their complaint.

There is a certain tension in the GDPR between provisions that fully recognise and embrace the realities of the single market, for instance by asserting the free flow of the free movement of personal data across internal EU borders, and provisions which are nevertheless made contingent on internal borders – as is the case, for example, in the rules applying to the competence of DPAs, which will be dependent on the territory of their Member State.

The GDPR provisions on complaints are also affected by this tension. On the one hand, data subjects are granted under Article 77 of the GDPR the possibility to lodge a complaint with potentially three different DPAs, and to freely choose between all the available options. On the other hand, however, much of the discourse surrounding the one-stop-shop appears to be grounded on the assumption that it is a problem, or a significant burden, for data subjects to enter in contact with the DPA of a Member State different from the one in which they are. An EDPB brochure, for example, presents the one-stop-shop by giving an example involving three Italian citizens whose personal data is processed by a Swedish company; '*thankfully',* says the leaflet, they can nevertheless lodge a complaint with the Italian DPA, and thus eventually contest the decision of the DPA in front of a court '*in their native language'*.[323]

Whereas proximity is certainly a very important factor in access to remedies, data subjects might wish to consider a variety of factors when deciding with which DPA to lodge a complaint. Taking into account that all DPAs must facilitate the online submission of complaints, they are actually all equally (non-)distant for data subjects in general. In the example mentioned, the data subjects might actually prefer to lodge with a DPA in a different Member State than the one of their residence if that would increase the chances of effective handling, regardless of the potential interest in taking a DPA to court in their native language.

The GDPR does not distinguish between 'domestic' or direct complaints and other types of complaints, but for the purpose of explaining the current situation it is possible to refer to complaints lodged with a DPA different from the DPA of the Member State of habitual residence as '**cross-border complaints'**.

4.5. Almost non-existent acknowledgment of the role of NGOs

Data subjects visiting DPAs websites in search of information on how to exercise their data protection rights are unlikely to encounter meaningful and useful information on their rights under Article 80 of the GDPR.

This state of play seems to ignore the potential of not-for-profit bodies, organisations and associations to contribute to strengthening the access to data protection remedies and GDPR enforcement.

In principle, NGOs could be of use at many levels. First, they could be of use as a first line of information for data subjects, providing general guidance that would allow the data subject to

[323] EDPB, *The EDPB: Guaranteeing the same rights for all ('One-Stop-Shop Leaflet'),* June 2021.

make (better) informed decisions about whether to lodge a complaint, and with which DPA. Second, they could assist during the submission procedure. Third, they could help data subjects situations where an effective remedy against the DPA is sought pursuant to Article 78 of the GDPR.

The EU legislator has recently agreed to impose on competent national authorities under the Data Governance Act (DGA)[324] the obligation to '*keep and regularly update a **public national register** of recognised data altruism organisations',*[325] and the European Commission '*shall keep and regularly update **a public register** of all data intermediation services providers providing their services **in the Union'***.[326] A similar register of entities qualified to represent data subjects in court or in front of DPAs could be established. It appears particularly timely to consider the possibility to devise either public national registers and/or an EU-wide public register of entities that fall within Article 80 of the GDPR.

5. Ways forward

In light of the problems identified, a number of options may be considered to improve access to remedies under the GDPR, in particular in relation to complaints. When considering future action, it is important to be mindful of the fact that improving access to remedies is not only crucial for the benefit of the individuals actively seeking remedies, but more broadly to improve GDPR enforcement. Not all data subjects whose rights need protection will take the steps necessary to lodge a complaint.[327] However, all would benefit from improved enforcement.

A key priority must be further **improving legal certainty and transparency about the handling of complaints lodged with DPAs**. Over the years, DPAs have been developing a variety of different approaches to complaint handling. These innovations are bringing an added level of confusion to a landscape which already lacked transparency for data subjects,[328] and demand a detailed exploration.

The 'fast-tracking' of complaints can have advantages in terms of efficiency.[329] Some procedures, however, may be problematic if they would distort the nature of complaints, and divert data subjects from the remedies to which they are entitled under the GDPR. The remedies under Article 78(2) are only available to data subjects after a complaint is lodged; **this remedy might be unavailable if a complaint is treated as 'withdrawn'** by a DPA, depending on how this takes place. Data subjects' complaints shall in any case not be treated as mere 'tips', but as real complaints.

---

[324] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L152.
[325] Art. 17(1) Data Governance Act.
[326] Art. 11(10) Data Governance Act.
[327] The European Commission noted in 2012 that '*Many individuals may have experienced detriment, but either resolved the issue with the data controller or did not pursue the complaint. Those that pursue a complaint are likely to have experienced significant harm'* (SEC(2012) 72 final, p. 29).
[328] Already in 2014, the FRA echoed that DPAs should be more transparent and communicate more effectively in order to ease access to remedies in practice (FRA, 2014, op. cit., p. 9).
[329] The European Commission has celebrated that 'amicable settlements' might spare DPAs resources (Answer given by Mr Reynders on behalf of the European Commission to Parliamentary Question ref. E-002629/2021, 23 July 2021).

Also importantly, inappropriate 'fast-tracking' could be at odds with the DPAs obligation to execute their responsibility for ensuring that the GDPR is **fully enforced, with all due diligence**. More clarity is thus needed on the limits of 'fast', 'light', 'soft' procedures for complaint handling together with the recognition that data subject's right to an effective remedy cannot be superseded.

Clarity about handling goes hand in hand with **improved metrics**, which must be based on harmonised or at least compatible definitions, **registration and reporting practices**. Knowing how many complaints are being lodged, and what occurs to them, is crucial to assess and improve GDPR enforcement.

Defining the best strategy for registration and reporting nevertheless requires a prior open discussion about what are the objectives of such practices. Leaving the definition of priorities completely in the hands of DPAs might lead to a situation in which statistical data offer only a partial picture of the phenomenon – illustrating for instance the burden represented by incoming complaints, without keeping track of other important aspects such as admissibility thresholds, delays in handling and nature of the outcome of complaints.

There is evidence of best practices among DPAs in relation to their obligation to **facilitate the submission of complaints**. DPAs should be encouraged to share and broadly adopt these practices. The EDPB might also consider to formally issue best practices, in line with its tasks.[330] Good practices identified include, for instance, clearly signalling a form for exercising the right to lodge a complaint with a visible button on the homepage; to automatically and systematically provide data subjects with proof of submission after the online submission of a complaint, which clearly indicates the exact date of submission; or to provide appropriate information about Article 78 of the GDPR after the submission of a complaint.

In addition, 'facilitating' the submission of complaints might be understood broadly, not as merely technically allowing the effective uploading of a complaint, but as putting in place practices that guarantee that the submission is a meaningful act, and that data subjects effectively have access to real remedies. **The minimal support currently offered is not in keeping with the role of DPAs as guardians of data protection enforcement.**

The '**cross-border lodging of complaints'** is currently generally not facilitated. Article 77 of the GDPR establishes that data subjects have the right to lodge complaints with the DPA of their habitual residence, the DPA of their place of work, or the DPA of the alleged infringement. Data subjects are thus given the possibility to choose, potentially, between three different DPAs. In practice, however, data subjects might not be able to exercise this right to choose, either because they have not been informed about its existence (even after reading all the information available on a DPA website), or because of obstacles complicating or rendering impossible the lodging of cross-border complaints. Most of the encountered problems stem from a lack of effort to visibly welcome non-domestic complainants, for instance by offering templates that would allow complainants to select their Member State of residence, as well as from technical choices that favour certain identification requirements that are difficult for non-residents to satisfy.

[330] The tasks of the EDPB include to issue *'best practices in order to encourage consistent application of this Regulation'* (Art. 70(1)(e) GDPR).

DPAs have a key role to play in making sure that data subjects can effectively exercise **all of their rights under Article 77 of the GDPR**. In addition, specialised not-for-profit bodies, organisations or associations could also be of particular help for data subjects to effectively have access to all their rights under Article 77 of the GDPR, including in cross-border scenarios, by making available their knowledge.

It should be explored whether the '**cross-border lodging of complaints'** should be more **actively promoted**. Encouraging data subjects to lodge complaints directly with the DPA which might otherwise become the lead supervisory authority in a one-stop-shop procedure, as opposed to with the DPA of their habitual residence, could have a positive impact on a variety of actors. It could possibly contribute to limiting the total number of cases which have to be subject to the one-stop-shop, a mechanism which is typically more cumbersome than the standard procedure, as it requires the involvement of multiple DPAs.

Data subjects should in any case benefit from having more information and being able to make a real informed choice. Such information could be provided by the DPAs themselves. Existing initiatives such as the European Consumer Centre (ECC), could be involved in this process. The ECC's mission is to deliver free information, advice and assistance on cross-border shopping, and helps consumers who have a problem with a trader based in a different Member State, Iceland or Norway for purchases made abroad, physically or online.

One of the main drawbacks for data subjects lodging complaints with a DPA other than the one of the Member State of their habitual residence is that in case they eventually wish to exercise their right to an effective judicial remedy against the decision of the DPA, they will have to exercise such right in a Member State different from the Member State of their habitual residence. The significance of this drawback could nevertheless be mitigated by better supporting specialised not-for-profit bodies, organisations or associations available to be mandated by data subjects wishing to exercise their right under Article 78 of the GDPR in such cross-border situations.

The GDPR marked an important step in the recognition of the role of not-for-profit bodies, organisations or associations in the enforcement of EU data protection law. DPAs, nevertheless, often fail to inform data subjects about their rights under Article 80 of the GDPR. It could be explored whether DPAs should be encouraged or mandated to provide information on **exactly which not-for-profit body, organisation or associations can be mandated by data subjects**, under the national law of their Member State, to exercise the rights referred to in Articles 77 and 78 on their behalf – for instance in national registers, or an EU-wide register. Alternatively, public listings could be made available by other stakeholders.

Such information might be provided on the websites of the DPAs, or alternatively by the EDPB or other EU institutions or bodies, or by civil society organisations supported for such purpose.

Finally, it should be examined how to monitor compliance by DPAs with their own obligations both in relation to complaint handling in general and in the context of their cooperation under Article 60. The role of the EDPB to make sure that DPAs '*reach a common understanding of the obligations entrusted to them by the GDPR*'[331] is crucial, but

[331] EDPB, *Internal Document 02/2021*, p. 11.

the question of how to make sure that in addition to understanding them, they consistently comply with them, remains open.

The EDPB has over the years progressively improved the transparency of its activities, which is laudable. Such a continuous effort should be sustained and further strengthened, also – crucially - in relation to EDPB work on data subject remedies, and most notably DPA obligations in relation to facilitating the submission of complaints and their handling, which directly touch upon Articles 8 and Article 47 of the EU Charter.

6. Concluding remarks

This study has provided an overview of current practices concerning access to remedies under the GDPR by combining legal analysis and empirical research, based on the observation of DPAs websites. The study offers pertinent materials in order to support more informed discussions as well as to inform future research. It highlights the potential and challenges of research in this domain. Two points stand out.

First, the study of DPAs practices – and the many ways in which these practices intersect with EU fundamental rights – is nowadays hindered by the limited availability of information about them. The annual reports that DPAs are obliged to produce (following a long-established tradition, dating from the very origins of European data protection law), are generally very useful, but other extremely valuable sources have proven much more difficult to access. This concerns, for instance, the questionnaires answered by EU DPAs in 2020 for the consultancy Milieu,[332] despite the fact that such data collection was financed by public funds. Some important documents related to the work of EU DPAs are currently available for the research community only thanks to the efforts of civil society organisations and their use of public access requests. Regrettably, some of the documents, they have obtained, have been partially redacted by DPAs, with answers to fundamental questions such as '*Does your SA investigate all complaints lodged with it*?' deliberately masked.

Given that the availability of such information would help to scrutinise the activities of DPAs with the ultimate aim of securing more effective data protection for EU residents, the DPAs and the EDPB must do more to embrace openness and further facilitate the public availability of all relevant information.

Second, the study has shown that to better understand the implementation and enforcement of the GDPR it is imperative to mobilise knowledge of both EU and national laws. This study clearly demonstrates how the procedures applicable at national level have the capacity to hinder the effective protection of EU Charter rights. These procedures therefore require further scrutiny which will necessarily touch upon a variety of fields of national law while also requiring attentiveness to the many languages and contexts in which the GDPR is applied in practice. This will demand additional efforts and cooperation from researchers, but it is scientifically valuable work. We hope this study will pave the way for further such future research collaborations.

[332] Access to the answered questionnaires for the purposes of this study was possible via the request for access to documents 2022-19, submitted by *noyb* to the EDPB (documents obtained in April 2022).

References

Agencia Española de Protección de Datos (AEPD), *Memoria anual 2018*, 2019.

--- *Memoria anual 2021*, 2022.

Autorité de Protection des Données (APD) – Chambre Contentieuse, *Politique de classement sans suite de la Chambre Contentieuse*, 18 June 2021.

Autoriteit Persoonsgegevens (AP), *Beleidsregels Prioritering klachtenonderzoek*, 2018.

--- *Jaarverslag 2018*, 2019.

--- *Jaarverslag 2019*, 2020.

--- *Jaarverslag 2020*, 2021.

Bieker, Felix (2022), *The Right to Data Protection Individual and Structural Dimensions of Data Protection in EU Law*, Asser/Springer.

Clifford, Damian and Yung Shin Van Der Sype (2016), 'Online dispute resolution: Settling data protection disputes in a digital world of customers', *Computer Law & Security Review,* Vol. 32, Issue 2, pp. 272-285.

Comissão Nacional de Proteção de Dados (CNPD), *Relatório de atividades de 2017/2018*, 2019.

--- *Relatório de atividades de 2019/2020*, 2021.

Commission nationale de l'informatique et des libertés (CNIL), *Dix ans d'informatique et libertés, Economica,* 1988.

--- *40e Rapport annuel 2019 : Protéger les données personnelles, Accompagner l'innovation, Préserver les libertés individuelles*, 2020.

--- *Rapport annuel 2021 : Protéger les données personnelles, Accompagner l'innovation, Préserver les libertés individuelles,* May 2022.

Courmont, Antoine (2022), *'« On a beaucoup de droits, ok, mais pour les faire valoir, c'est compliqué » : les épreuves de l'exercice des droits',* LINC/CNIL, 25 February 2022, https://linc.cnil.fr/fr/beaucoup-de-droits-ok-mais-pour-les-faire-valoir-cest-complique-les-epreuves-de-lexercice-des-droitshttps://linc.cnil.fr/fr/beaucoup-de-droits-ok-mais-pour-les-faire-valoir-cest-complique-les-epreuves-de-lexercice-des-droits

Data Protection Commission (DPC) *Annual Report - 25 May - 31 December 2018*, 2019.

---- *One-Stop-Shop Cross-Border Complaint Statistics, 25 May 2018 – 31 December 2021*, 2022.

--- DPC, *Annual Report 2021,* 2022.

Datenschutzbehörde (DSB), *Datenschutzbericht 2018,* 2019.

--- *Datenschutzbericht 2019,* 2020.

--- *Datenschutzbericht 2020,* 2021.

--- *Datenschutzbericht 2021,* 2022.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, *30. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit 2021*, April 2022.

European Commission (EC), *Analysis and impact study on the implementation of Directive EC 95/46 in Member States*, 2003.

--- *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee, and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union,* COM(2010) 609 final, Brussels, 4.11.2010.

--- *Impact Assessment,* Commission Staff Working Document accompanying COM(2012) 10 final, COM(2012) 11 final, SEC(2012) 73 final, SEC(2012) 72 final, Brussels, 25.1.2012.

--- *Implementation and transposition of Articles 85 and 78 GDPR and Article 53 LED: Overview of discussions with the members of the GDPR/LED expert group*, November 2021.

--- *April infringements package: key decisions*, 6 April 2022.

European Commission's Expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, *Questions for the GDPR/LED Member States Expert Group*, May 2021.

European Data Protection Board (EDPB), *Rules of procedure,* Version 8, adopted on 25 May 2018, as last modified and adopted on 6 April 2022.

--- *Annual report 2018: Cooperation and transparency*, 2019.

--- *First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities,* 2019.

--- EDPB, *Info Note: Cooperation subgroup, Outline – The practical implementation of the amicable settlement,* 25 September 2019 (Document 34 of request for access to documents 2022/27, submitted by Johnny Ryan to the EDPB (documents obtained in May 2022).

--- *Annual report 2019: Working together for stronger rights*, 2020.

--- *Contribution of the EDPB to the evaluation of the GDPR under Article 97*,

adopted on 18 February 2020.

--- *Internal EDPB Document 06/2020 on preliminary steps to handle a complaint: Admissibility and vetting of complaints,* adopted on 15 December 2020.

--- *Handling cross border complaints against public bodies or authorities,* document without date, probably dated 2021 (a request for mandate is mentioned in the Agenda of the 43rd EDPB meeting of 15 December 2020), Document 89 of request for access to documents 2022-19, submitted by *noyb* to the EDPB (documents obtained in April 2022).

--- *Annual report 2020: Ensuring data protection rights in a changing world,* 2021.

--- *Internal EDPB Document 02/2021 on SAs duties in relation to alleged GDPR infringements,* Version 1.0, adopted on 2 February 2021.

--- *45th Plenary meeting 2 February 2021 (Remote),* 2021.

--- *The EDPB: Guaranteeing the same rights for all* ('One-Stop-Shop Leaflet'), June 2021.

--- *Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities*, August 2021.

--- *Internal EDPB Document 06/2021 on the practical implementation of amicable settlements*, adopted on 18 November 2021.

--- *Guidelines 02/2022 on the application of Article 60 GDPR*, Version 1.0, adopted on 14 March 2022.

--- *Statement on enforcement cooperation,* adopted on 28 April 2022.

--- *Agenda of 65th EDPB meeting, 12 May 2022, Remote,* 2022.

--- *Guidelines 06/2022 on the practical implementation of amicable settlements*, adopted on 12 May 2022.

European Data Protection Supervisor (EDPS), Opinion 3/2015, *Europe's big opportunity, EDPS recommendations on the EU's options for data protection reform,* 2015.

European Parliament, *Resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application* (2020/2717(RSP).

European Union Agency for Fundamental Rights (FRA), *Access to data protection remedies in EU Member States,* 2014.

Gegevensbeschermingsautoriteit (GBA), *Jaarverslag 2018,* 2019.

--- *Jaarverslag 2019*, 2020.

--- *Jaarverslag 2020*, 2021.

González Fuster, Gloria (2020), 'Article 80', in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020), pp. 1142-1152.

Hellenic Data Protection Authority, *Ετήσιες εκθέσεις* 2018, 2019 and Summary of Annual Report 2018, 2019.

--- *Ετήσιες εκθέσεις* 2019, 2020, and Summary of Annual Report 2019, 2020.

--- *Ετήσιες εκθέσεις* 2020, 2021.

Irish Council for Civil Liberties (ICCL), *Europe's enforcement paralysis: ICCL's 2021 report on the enforcement capacity of data protection authorities*, 2021.

Jančiūtė, Laima (2019), 'Data protection and the construction of collective redress in Europe: exploring challenges and opportunities', *International Data Privacy Law*, Volume 9, Issue 1, February 2019, pp. 2–14.

Kantor Management Consultants (2007), *Evaluation of the Means used by National Data Protection Supervisory Authorities in the promotion of personal Data Protection: Final report*.

Korff, Douwe and Ian Brown (2010), *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments,* European Commission.

Milieu, *Study on the national administrative rules impacting the cooperation duties for the national supervisory authorities: Questionnaire for the national supervisory authorities* -as completed for *Austria, Belgium, Cyprus, Hungary, Netherlands, Lithuania, Luxembourg, Slovak Republic*, EDPS/2019/02-07, February 2020 as made available in the context of request for access to documents 2022-19, submitted by *noyb* to the EDPB (documents obtained in April 2022).

Petroiu, Marius (2018), 'Romania: overview of the GDPR implementation', *European Data Protection Law Review (EDPL*), 4(3), pp. 366-369.

Ramón-Díaz, Alonso (2022), 'La inadmisión a trámite de las reclamaciones presentadas ante la Agencia Española de Protección de Datos', *Diario La Ley*, No 9985, Sección Tribuna, 10 de enero de 2022, Wolters Kluwer.

Revolidis, Ioannis (2017), 'Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of"Privacy Tourism"?', *Masaryk University Journal of Law and Technology* 11(1), pp. 7-37.

Valstybinės Duomenų Apsaugos Inspekcijos, *2021 Metų Veiklos Ataskaita*, 2022 m. kovo 7 d. Vilnius.

Van Rompuy, Peter, *Schriftelijke vraag nr. 7-287, aan de minister van Digitale Agenda, Telecommunicatie en Post, belast met Administratieve Vereenvoudiging, Bestrijding van de sociale fraude, Privacy en Noordzee*, Belgische Senaat, 17 januari 2020.