By e-mail to:

The European Data Protection Board and its members (edpb@edpb.europa.eu)

Brussels, 2 September 2022

Subject: Invitation to meet the EDPB on 13 September 2022 to discuss procedural aspects of the enforcement of the GDPR

Dear Chair Dr. Jelinek,
Dear members of the EDPB,

EDRi and its members thank the European Data Protection Board for its invitation to meet and share with its members the procedural aspects of the General Data Protection Regulation that, in our views, should be addressed and potentially harmonised to achieve a better enforcement of the law.

Concerns about the lack of effective enforcement of the GDPR have already been shared by EDRi and its members in various letters and reports to which we would like to refer, before sharing further concerns regarding specific procedural aspects as requested by the EDPB:

- *noyb* comments on the enforcement of the GDPR, letter to the Commission at staff level, 28 June 2021;
- Civil society call and recommendations for concrete solutions to GDPR enforcement shortcomings, letter from EDRi to the EDPB, the LIBE Committee and the European Commission, 16 March 2022;
- The right to lodge a data protection complaint: ok, but then what?, an empirical study of current practices under the GDPR by the Data Protection Law Scholars Network (DPSN), published in June 2022 and commissioned by Access Now; and
- Four years under the GDPR: How to fix its enforcement, published in July 2022 by Access Now.

In the documents mentioned above[1], EDRi and its members have already identified several problems with the enforcement of the GDPR as well as possible solutions to address them. We

[1] We would also like to refer to the 2020 report from BEUC: "Two years of the GDPR: A cross-border data protection enforcement case from a consumer perspective" where BEUC already pointed several issues and recommendations mentioned in this letter: https://www.beuc.eu/sites/default/files/publications/beuc-x-2020-074_two_years_of_the_gdpr_a_cross-border_data_protection_enforcement_case_from_a_consumer_perspective.pdf

invite the EDPB to take these into consideration when assessing possible avenues for improving the enforcement of the GDPR.

In this context, we note that the EDPB invited EDRi and its members to share a “single and consolidated list of procedural aspects that, in your view, could be further harmonised in EU law”. EDRi members consider that the issues linked to the lack of effective enforcement of the GDPR go beyond the lack of harmonisation of procedural laws. Limiting discussions to this single aspect would imply, indeed, that only cross-border cases requiring cooperation between Supervisory Authorities require improvement from an enforcement point of view. However, EDRi members have also observed multiple national cases where GDPR complaints and violations were not properly addressed by the Supervisory Authorities. In those cases, this was not caused by a lack of harmonisation of national procedural laws, but by several other factors, such as – among others - a lack of resources, refusal to act upon a complaint, unexplained delays in dealing with a complaint, absence of any update on the status of the complaint, or difficulties in filing a complaint with the relevant SA.

For these reasons, we are concerned that the discussions on the effective enforcement of the GDPR only focus on the lack of harmonised procedures and we invite the EDPB to extend the scope of its work when addressing the shortcomings with the enforcement of the GDPR. We, however, understand that the EDPB cannot solve all the issues regarding the enforcement of the GDPR and has limited competences and powers.

Therefore, to assist the work of the EDPB in comprehensive addressing of the problems with the enforcement of the GDPR at national and cross-border level, we present the following two-fold methodology:

- **First**, identifying the problems leading to a non-effective enforcement of the GDPR, both at national and cross-border level. This would ideally refer to specific cases where recurring problems can be identified. A consensus should be reached on the list of various problems to be addressed to achieve a better enforcement of the GDPR. Findings from our members' reports referenced above can be used for these tasks.
- **Second**, propose and debate different solutions that could potentially solve the problems identified under the first step.

In this context, while we acknowledge that the lack of harmonisation of national laws is one of the obstacles to an effective enforcement of the GDPR, we invite the EDPB (and potentially the Commission) to open the dialogue to other potential issues to be solved.

As requested by the EDPB and to further guide the tasks proposed in our two-step methodology, we prepared a consolidated table referring to the problems we have identified, the suggested solutions and some further explanations when needed. However, at this stage, we considered it premature to share any drafting suggestions since the nature of the document where such drafting suggestions would be incorporated (*e.g.* EDPB guidelines, legislative initiative, or recommendation) was not clear to us.

We grouped the different problems identified by subject for the sake of readability of the table. The last column of the table and footnotes refer to specific cases encountered by EDRi members to make the discussion more specific.

While we aimed to be as comprehensive as possible, we acknowledge that the EDPB and its members may be aware of additional issues with the enforcement of the GDPR that are not referred to in this table. Likewise, we did not order them by priority in this table and we therefore leave it up to the EDPB and its members to select the most pressing issues that they may identify.

We look forward to exchanging further on these issues during our upcoming meeting and to cooperating with the EDPB and its members to develop solutions to improve the enforcement of the GDPR.

Sincerely,

Access Now
noyb
European Digital Rights (EDRi)

Bits of Freedom, The Netherlands
Dataskydd.net, Sweden
Državljan D / Citizen D, Slovenia
Elektronisk Forpost Norge, Norway
Homo Digitalis, Greece
La Quadrature du Net, France
Panoptykon Foundation, Poland
Asociația pentru Tehnologie și Internet – ApTI, Romania
epicenter.works – for digital rights, Austria

Problems identified	Suggested solutions	Concrete case – illustration – reference – link
Topic 1 - FILING OF A COMPLAINT		
Lack of harmonised and unique complaint form	A common complaint template should be decided for all SAs in all languages used by the SAs.	
Lack of information on access/ accessibility to the SA and the relevant page to file the complaint (finding the right SA, general lack of awareness)	EDPB should make available 1 single online page with practical information for data subjects to know which DPA they can contact, with links to all DPAs and their specific pages for submitting complaints. It could also be an interactive page in which the data subject states where they live/work, where they believe the controller/processor are established, etc, and the page gives the different possibilities.	https://www.accessnow.org/cms/assets/uploads/2022/07/GDPR-Complaint-study.pdf, page 51
Lack of clarity on the website on where to send a complaint or how	Each SA should provide a link to a harmonised form to file a complaint on the first page of their website with a clearly noticeable icon/section called “file a complaint”.	https://www.accessnow.org/cms/assets/uploads/2022/07/GDPR-Complaint-study.pdf p-39 to 43
Complaint forms do not always provide the possibility to send all attachments and evidence Some SAs do not allow submitting more than a certain amount of attachments or files above a certain size, which limits the complainant who wants to attach evidence or other relevant documents to the complaint.	The EDPB should make available one single online page with practical information for data subjects to know which SA they can contact, with links to all SAs and their specific pages for submitting complaints. It could also be an interactive page in which the data subject states where they live/work, where they believe the controller/processor are established, etc, and the page gives the different possibilities. This page could be promoted so data controllers can link to it in their data protection notices.	
Not always possible to send complaints or to communicate with the authorities by email NGOs sending complaints usually use the same template or submit multiple complaints and it would be easier to send these complaints to dedicated email addresses where complaints can be sent.	SAs should guarantee they facilitate the submission of complaints also by making sure that all relevant documents for the complaint can easily be shared with the SA, for instance by submitting it through different means (*e.g.* an email address where complaints and attachments can be sent, or a form allowing to attach any electronic format without maximum number of attachments).	

Loss of complaints After having sent a complaint, the complainants do not always receive an acknowledgement of receipt.	SAs should always send an acknowledgement of receipt of the complaint with a reference number.	In some cases (e.g. Bulgaria), the SA stated that no complaint was received, whereas an email was sent and indicated as "read" by the recipient.
Different criteria to file a complaint depending on the country The same complaint filed in different countries can be accepted by some SAs but rejected by others on different grounds (lack of residency in the country of the SA, not sending a prior request to the controller, lack of identification of legal grounds in the complaint).	All SAs should apply the EDPB guidelines on admissibility criteria. Besides, existing national rules should be examined by the Commission to make sure that they do not conflict with the GDPR. The complainant should not be required to identify the specific legal grounds in the complaint since this makes it an obstacle to file a complaint for non-lawyers. SAs should have a clear list of minimum elements to be mentioned in the complaint and reflect it in the complaint form (e.g. indicating if the information is necessary or not). In case an SA considers itself not competent to handle a complaint, the legal reasons for that should be expressly mentioned. SAs should investigate GDPR aspects, even if ePrivacy falls within the competence of another authority.	See: https://www.accessnow.org/cms/assets/uploads/2022/07/GDPR-Complaint-study.pdf pages 43 to 48
When the SA is not competent (no territorial jurisdiction or not competent for another reason) the SA does not always refer the complainant to the competent authority In such cases, the complainants might not know where to redirect their complaints.	SAs should always send a complaint to the competent authority and inform the complainant about this action so that they do not have to guess what the competent authority is.	See case in Spain where the AEPD rejects its competence on the ground of the ePrivacy Directive but does not refer the case to the competent authority, despite a clear obligation to do so under the ePrivacy Directive (*noyb*'s IDFA case).

Language and administrative barriers to lodge a complaint across the EU - In certain cases, the complaint (including all the attachments) can only be filed in one official language of the SA although the complainant actually has the right to choose a language that the SA understands and could use in the cooperation procedure. - Some SAs require an e-Gov access to file a complaint or even to communicate electronically with the complainant, which does not allow people without such e-Gov access (like NGOs not established in the country) to file the complaint under the same conditions as nationals with an e-Gov access. Additionally, the electronic communication systems using e-Gov often impose a limit on the number of files that can be attached per one message or even on the permitted formats of the attachments. - Not all Member States recognise official electronic signatures of other MS resulting in SAs dismissing the complaint. -	There should be a possibility to file a complaint in different languages (English, for example) than just the language used by a SA (usually the official language where the SA is established). Ensure that e-Admin or e-Gov platforms that may be used to send and receive complaints do not limit data subjects' rights to lodge complaints: data subjects should not need to have an ID card, e-access or registration number from a certain Member State to be able to exercise their rights. The electronic communication system (if it is not e-mail) should allow for multiple attachments in various formats. SAs should accept e-signatures from other Member States in line with the applicable law. SAs should be transparent in their answers to the EDPB regarding this matter (the answers from SAs were redacted in the document received after a request for access to the relevant documents).	See https://www.accessnow.org/cms/assets/uploads/2022/07/GDPR-Complaint-study.pdf pages 45-49 as well as 59 and 60 See, for example, the situation in Spain where an NGO cannot correspond with the AEPD without an e-certificate.
Topic 2 – PROCEDURE AFTER THE COMPLAINT HAS BEEN FILED		
Update on the progress of the complainant - In most cases, complainants do not receive regular updates from the SAs at all, even several months and sometimes years after filing the complaint, and despite several reminders. - It is further unclear which SA is required to provide an update, since	The CSA receiving the complaint should be the one informing the complainant. This information should be done in the language used in the complaint. The update should not only happen once after 3 months as stated by the EDPB but regularly, as Article 77(2) obliges the SA to inform the complainant on any progress and outcome of the complaint. An update every 3 months (as practiced e.g. by some SAs) would allow a	See https://noyb.eu/sites/default/files/2022-03/Follow-up%20meeting_Redacted.pdf, Section 1.1.f

Article 77(2) requires the SA "with which the complaint has been lodged" to provide information but Article 78(2) addresses the SA "which is competent pursuant to Articles 55 and 56". - Oftentimes the CSA receiving the complaint acts as a pure mailbox and transfers the updates from the LSA in the language of the LSA which is usually not the language of the complaint and the procedure.	complainant to know that their complaint is still being handled. The information shared with the complainant should be substantial and mention at least the expected timeline for the decision, the reasons for the delay, the next procedural steps, and the possibility for the complainant to share their views. The CSA should provide a case number (including IMI number) and contact details of the case officer that the complainant can reach out to for updates to prevent the complainant being left in the dark.	
Judicial remedy in case the SA does not inform the complainant as per Article 78(2) GDPR Even though the GDPR provides for the right to an effective judicial remedy in case the SA does not inform the complainant, it is not clear what result can be expected from such a remedy. It seems that, in the absence of updates on the status of a complaint, the only thing that a complainant may request the court to do is to order the SA to inform the complainant as per Articles 77(2) and 78(2) GDPR. It is possible that such information will merely contain a notification that nothing happened since the last update communicated to the complainant, should there be any. Therefore, the whole judicial remedy amounts to substantial costs, energy, and time spent to achieve a result that does not really have an impact on the procedure or remedy the inaction of the SA.	It seems questionable that Article 77(2) GDPR has any real value unless it is clarified that the LSA and the CSA have a duty to produce information jointly, SAs must give complainants substantial information, and courts require such substantial information under Article 78(2) GDPR.	In a case against Netflix, *noyb* had to file judicial reviews with the Austrian Federal Administrative Court against the Austrian SA (CSA), because both the Dutch SA (LSA) and the Austrian SA failed to provide any substantial update for years. After these two judicial reviews, the Austrian SA finally gave an update. The effort made to simply receive an update in the case was immense.
Duty to decide on a complaint We observe an increasing number of SAs taking the view that they have no obligation	It should be made clear that all complaints should be followed by a formal decision, either rejecting or upholding the complaint, but always subject to appeal as per Article 78(1) GDPR.	See https://noyb.eu/sites/default/files/2022-03/Follow-up%20meeting_Redacted.pdf, Section 1.1.d

to adopt a binding decision after a complaint.[2] SAs have the obligation to handle all complaints. Amicable resolution and other "soft" handling results have sometimes an unclear status: all SAs should reach final decisions subject to appeal, in line with the right for complainants to an effective judicial remedy. However, some SAs issue "outcome" letters or non-binding decisions the status of which is not clear to the complainant.[3]	The fact that the decision is final and is subject to appeal should always be mentioned in the decision.	
Article 78(2) does not define what "not handling a complaint" means Some SAs also take the view that they must indeed handle a complaint, but that "handling" can mean just closing cases without any further investigation and without giving any reasons. Some SAs also argue that complainants have no right to appeal a decision to close a case, as SAs do not have a duty to act anyway. Following this line of arguments, the judicial review provided for in Article 78 would only exist when the SA has not informed the complainant on the progress (which is usually a mere information that the complaint is still "open", see below), and not when the SA remains inactive. That is because handling a complaint is not defined.	To ensure that Article 78(2) of the GDPR provides for an effective judicial remedy, it is crucial to provide a clear definition of what "handling a complaint" means.	https://www.accessnow.org/cms/assets/uploads/2022/07/GDPR-Complaint-study.pdf page 56 See https://noyb.eu/sites/default/files/2022-03/Follow-up%20meeting_Redacted.pdf, Section 1.1.e
Review of the courts under Article 78 GDPR What can be requested before a court in case the SA does not handle the complaint under Article 78(2)? This is unclear, among	It should be clarified, what can be requested from the court under Article 78 GDPR. The complainant should have an effective judicial remedy as per Article 78 and the court should exercise full jurisdiction under Recital	

[2] This view was publicly expressed by the Irish SA. A similar attitude from the LUX SA, refusing to adopt a final decision, is currently subject to a lawsuit in Luxembourg before an administrative court.
[3] See, for example, the Irish SA that can provide advice to the complainant under Section 109(4) of the Irish Data Protection Act, but not a formal binding decision.

others, because the national procedures and the competence of the courts are different.	143 GDPR. This should become a reality since in practice, courts are reluctant to substitute their views for the (sometimes non-existing) view of the SAs. In one stop shop cases, it should also be possible, for example: - to force the CSA receiving the complaint to act (investigate, address a request for cooperation under Article 60, take a decision on the admissibility of the complaint, or on the LSA) - to order an SA to adopt a decision under Article 66 if the case is not moving fast enough - to order the SAs to adopt a decision under Article 56) - to compensate the complainant for damages if the delay to handle the complaint is not duly justified by the SA.[4]	
Lack of deadlines to adopt a decision, or take any intermediary steps (investigation, rejecting the complaint, sending it to another SA) - Some complaints have been pending for 4 years (date of application of the GDPR) and the complainants are still waiting for an update, an investigation, or a decision. - Having seen the uncertainties of the procedure in front of some SAs, some complainants and civil society (*e.g. noyb*) are turning to courts to enforce the GDPR instead of the SAs, since civil proceedings give some	Establish clear deadlines for each step after a complaint has been filed. After receiving a complaint, the SA should quickly take a formal decision on: - the admissibility of the complaint - the competence of the SA or of another SA - the opening of an investigation or not - a timeline for the further steps.[5] Provide for the possibility to sue an SA for not being able to show any progress on the complaint. The SA should be accountable and be obliged to show that some action has been initiated regarding the complaint.	Among many other examples: It took 11 months to state that the Irish SA might not be competent on the cookies complaint.[6]

[4] The Brussels Tribunal held that the Belgian SA improperly handled the case of a complainant and committed a breach of its duty of care by not handling his amicable resolution request within a reasonable period of time. See: https://gdprhub.eu/index.php?title=Trib._Civ._Bruxelles_-_2021/2476/A

[5] For example, the Maltese SA automatically informs the complainants of the next procedural steps to be expected.

[6] See *noyb* cookies complaints: C-037-10028; C-037-10319; C-037-10445; C-037-10517; C-037-10753; C-037-11008; C-037-11143; C-037-11200; C-037-11432; C-037-12140; C-037-602; C-037-224; C-037-312; C-037-208; C-037-213; C-037-106; C-037-306; C-037-210 where the SA took 11 months to adopt a statement on the admissibility of the complaints. See also LUX SA deciding more than 14 months after the complaint was filed that the "101 complaints" should be dismissed since the website stopped using the service a couple of weeks after the filing of the complaint.

guarantees in terms of transparency and rights of the parties despite the disadvantages of court proceedings (financing, expertise, obligation to hire a lawyer). This situation is in tension with the objective of the GDPR which is reinforcing - rather than complicating - access to effective remedies, also for civil society.		
Topic 3 – COOPERATION PROCEDURE AND ONE-STOP-SHOP PROCEDURE		
Establishment of the competence of the LSA - Some procedures take years before even the start of the actual investigation on the complaint, and before the SA adopts a decision on the merits of the case. - In some cases, before continuing the procedure, the complainant is asked to confirm where the main establishment is. But in other cases, the complainant is not even invited to be heard by the EDPB when a question under Article 65(1)(b) of the GDPR arises. - In some cases, the complaint is sent by the CSA receiving the complaint to the potential LSA, from which the complainant does not receive any update on the matter.	SAs must actually assess questions of controllership and main establishment and not just accept a controller's declaration if the complainant raises substantiated doubts. SAs should issue a formal decision on competence that can be challenged before the courts. When the SAs do not agree on the competent LSA, the complainant should be informed on the matter and be able to trigger Article 65(1)(b) of the GDPR and ask for a decision by the EDPB itself since in many cases SAs remain inactive when they disagree on the LSA. The complainant should be given the IMI number of the case and the competent authority to which the complaint has been sent.	See *noyb* cases C001[7], C014[8] and C026[9] See https://www.accessnow.org/cms/assets/uploads/2022/07/GDPR-4-year-report-2022.pdf (Recommendations to SAs)

[7] Case on forced consent by Google when the French SA adopted a partial decision on the complaint and then sent the case to the Irish SA which then considered that it was after all not the LSA and sent it back to the French SA. The case was sent to the EDPB to determine the competent LSA four years after the complaint. Today, it is still not clear to the complainant (*noyb*) what the status of its complaint is.

[8] This complaint concerns a simple access request regarding YouTube and has been pending since January 2019. *noyb* is of the view that Google LLC is the relevant controller. Despite this, the Austrian DPA with which the complaint has been filed, has forwarded the case to the Irish SA as (assumed) LSA and the Irish SA refuses to act unless *noyb* accept their view that Google Ireland Ltd. is the controller. The result is that neither SA is doing anything.

[9] The situation here is similar to the one mentioned in the footnote above: *noyb* considers Google LLC to be the controller, the Irish SA refuses to act unless *noyb* accepts their view of Google Ireland being the controller. Neither the Austrian nor the Irish SA have conducted an investigation on the actual controllership, but after almost a year the Austrian SA decided to forward the case to the Irish SA as the assumed LSA.

- In other cases, the complaint is simply lost: the SA having received the complaint pretends to have it sent to the LSA and the LSA states that it did not receive the complaint. The complainant is left in a Kafkaesque situation.		
Language barriers/translations. - When a complaint filed with an SA is sent to the LSA, the LSA investigates and may adopt draft reports and documents that are shared with the complainant for them to send their submissions. However, some SAs do not translate the correspondence from the LSA and therefore do not allow the complainant to answer in the language of their complaint/procedure. - When translation is provided, it is often of poor quality. It is therefore difficult to answer and meaningfully argue the case if the translation of the other party's submission is incomprehensible.	The SA receiving the complaint should translate the documents received by other SAs to the language of the complaint or the preferred language of the complainant. SAs should check the preferred language of the complainant and translate all documents of the procedure/complaint to ensure that the complainant is able to understand and respond. There should be a minimum standard for quality control of the translations.	In the final decision published in the EDPB Art. 60 Register for EDPB:UK:OSS:D:2019:35 (decision of the Austrian SA), p. 3: this sentence can be read: "Pursuant to Art. 60 para. 8 GDPR, the supervisory authority with which the complaint was filed decides if a complaint is rejected or rejected." This sentence seems to have been obtained using automated translation software (GE to EN) and copied without verification. It is unclear why the very text of the GDPR is being incorrectly translated, despite it being publicly available in all languages.
Application of different procedural laws. The differences of national procedural laws are a problem for national cases but also cross-border cases. Indeed, the rights of the complainant depend on where the complaint is filed but also on the procedural laws of the LSA. The status of the complainant is not the same before every SA regarding, among other things: - access to the case file (see below) - the right to send submissions (see below) - the right to receive a formal binding decision (see above)	As a general solution, some common principles regarding the procedure before the SAs should be defined and applied in all national and cross-border cases. In order to achieve this, the following steps are suggested: - Research should be conducted on the divergences of national laws being an obstacle to the effective enforcement of the GDPR. - The Commission should propose legislation to complement the GDPR to ensure its harmonised application on a procedural level. In this context, the following elements should be taken into account:	See: https://www.accessnow.org/cms/assets/uploads/2022/07/GDPR-Complaint-study.pdf and https://www.accessnow.org/cms/assets/uploads/2022/07/GDPR-4-year-report-2022.pdf

	- As noted in EDPB guidelines[10], with respect to the EU principle of procedural autonomy and its limits, the primacy of EU law means 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**". - Harmonisation of procedures should cover specific steps to **ensure the effectiveness of data subjects' rights under the GDPR**. This harmonisation should focus on information they receive when doing so and the next steps, rights to be heard and to access documents related to one's complaints. This harmonisation should also set clear deadlines for each step of data protection complaints. - Procedures must be **harmonised to the top**, providing data subjects with the highest level of procedural rights that exist to avoid lowering data subjects' rights. For instance, even if only some Member States provide a right to be heard to the complainant, this shall be extended to all data subjects in the EU to provide people with equal rights while not lowering remedial rights.	
Member States have divergent approaches particularly in terms of **access to the documents** of the case file. Article 41 of the Charter provides for a right to good administration, which includes the right to have access to documents. However, we have observed that the SAs do not consistently answer requests for access to the file relevant to the procedures in which we are involved:	The right to have access to the documents of the procedure should be established in all countries. Specific rules for strict cases where confidentiality is established can exist but should always take into account the right to be heard by the other party to the procedure. The complainant should be able to access all documents to rebut the submissions of the controllers and processors.	

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

- Some SAs enable the parties to get access to the documents of the case only upon an in-person appointment in the offices of the SA. Upon request to get access to the documents of the procedure electronically, the complainant is rejected and is left without a possibility to be heard on the findings of the investigation before a decision is made by the SA.[11] - Moreover, some SAs unilaterally decide that some documents or parts of documents should be confidential, sometimes even without a clear legal basis.[12] - In any case, in case of appeal (Article 78 GDPR), the entire file will have to be shared with the parties to the judicial procedure. Therefore, raising the argument of confidentiality at the administrative stage does not make much sense.		
With regard to the **right to be heard**, the approach of SAs varies as to the extent of this right. - Some SAs only allow submission on the "facts", but not on legal arguments. - Some SAs do not hear the complainant at all, or decide on a case by case basis. - Some SAs do not hear the complainant if an "ex officio" investigation is open.[13] - Some SAs make the access to the file and the right to be heard dependent on the signature of an NDA (e.g. the Irish SA). - Some national procedural laws explicitly provide for a right to be	The complainant should always be heard, as this is a general principle of good administration and considering that the EDPB and the national and EU courts procedures allow for a full access to documents in an adversarial procedure. The right to be heard should also be observed where a case is sent to the EDPB, since the Rules of Procedure and guidelines of the EDPB require the Secretariat to verify that the right to be heard has been respected before considering that the file is complete. Only giving this right to the complainant at the EDPB level gives an advantage to the controller that was able to bring arguments before the LSA without the complainant being able to rebut them.	

[11] This is the case in Poland.
[12] See, for example, the Irish SA or the EDPS.
[13] See *noyb* case https://noyb.eu/en/data-breach-malta-65000-eu-fine-c-planet.

heard at national level but ignore this when the case is cross-border and refuse to share documents and to give the opportunity to be heard.		
No clarity about what information to share with the CSAs during the cooperation phase under Article 60 GDPR Some LSAs do not share all the documents of the case (but rather only a summary/overview of some of the documents) with the CSAs. That could leave out some aspects of the procedure or some arguments made by the parties, which can therefore not be considered by the CSAs having to express reasoned objections.	The LSA should inform the CSAs on the different stages of the procedure throughout the entire drafting process of the draft decision. The LSA should proactively share information about progress in case and not wait for a draft decision to be completed so that the CSAs can ask to correct the scope if necessary.	
The cooperation between SAs is too minimal The possibility for SAs to cooperate, start joint investigations, and ask for information is not really used in practice. The scope of the complaint/investigation is usually left to the LSA in the draft decision, and the rare requests from the CSAs are usually ignored.	SAs should use the cooperation mechanisms such as mutual assistance and joint operations, especially when the LSA is not acting. The complainant should be able to ask the competent court under Article 78 GDPR to order an SA to ask other SAs to answer requests under Article 60, 61 and 62 GDPR. LSAs should consult CSAs to define scope of a case and follow. Article 66 GDPR should be automatically triggered when an SA is not replying to requests (see Articles 61(8) and 62(7) GDPR.	
Coordination of decisions (within or outside the one-stop-shop) Some similar or identical cases receive a different outcome from different SAs even when the case is cross-border. The coordinated efforts of the SAs do not have the same outcome (decisions, cease and desists, dismissal of the complaint).	In cross-border cases, but also in other cases, when multiple similar complaints are pending about a controller company, there should be an obligation to jointly investigate (or create a task force at the EDPB level) and reach joint position but also a similar outcome (sanction, dismissal, or rejection of the complaint).	See the Grindr decisions from the Norwegian SA and the Spanish SA not agreeing on the definition of sensitive data. See the different outcomes of the SAs after the coordination at the EDPB level on *noyb*'s 101 complaints regarding cookie banners. *noyb*'s 101 complaints:

		SAs of Austria, France and Italy found a violation (unlawful EU-US data transfers) at a certain point. SAs of Luxembourg and Spain dismissed the case, because a controller stopped using tools causing the transfers, without taking a decision on whether there had been a GDPR violation.
Absence of a deadline within the cooperation mechanism In many cases, the absence of provisions imposing a specific deadline in the GDPR make it difficult to get a draft decision under Article 60 GDPR within a reasonable period.	Timelines should be determined with respect to: - the transfer of complaints to the LSA (in some cases, CSAs only forward the complaint several months after the complaint was lodged); - the start of an investigation (in some cases the LSA started the investigation years after having received the complaint from the CSA); - the adoption of a formal decision on the designation of the LSA (in several cases, we are not even informed of the designation of the LSA and we do not know how we can challenge this decision before a final decision on the merits is adopted); - the issuance of a draft decision "without delay" under Article 60(3) GDPR; - the time to submit a revised draft decision under Article 60(5) GDPR.	
No use of the emergency procedure The emergency procedure under Article 66 GDPR is rarely used[14] and the possibilities to trigger Article 66 GDPR in cases where urgency is presumed under Articles 61(8) and 62(7) GDPR is not used in practice.	SAs should be obliged to use emergency procedures in cases referred to by Articles 61(8) and 62(7) GDPR. The complainants should be able to ask for an urgent decision under Article 66(1) GDPR and Articles 61(8) and 62(7) GDPR. The SA should justify the reasons why it refuses to issue a decision under this Article.	https://www.accessnow.org/cms/assets/uploads/2022/07/GDPR-4-year-report-2022.pdf See https://noyb.eu/sites/default/files/2022-03/Follow-up%20meeting_Redacted.pdf, Section 1.1.j.
Topic 4 – DISPUTE RESOLUTION AT EDPB LEVEL UNDER ARTICLE 65 GDPR		
Right to be heard at the EDPB level	The Rules of Procedure should provide clearly that both the controllers and the complainants	

[14] The sole example of such decision that we are aware of is the use of article 66 by the Italian SA: https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_-_9574709.

The complainant should always be heard at the EDPB level under Article 41 CFR. Complaintants should also have a right to be heard before all SAs. Additionally, the fact that the complainant was or could have been heard at the national level is not enough since the EDPB is a different organ and the decision and arguments are not the same as in the national procedure. This right also includes the right to access all documents of the procedure by the complainant. The fact that some SAs refuse to give access to the file during the national procedure and only share the documents with the controllers puts the complainant in a disadvantageous position compared to the controllers since they were not in a position to submit their position at an earlier stage.	must be heard by the EDPB (at least by giving the complainant the possibility to share written submissions). Access to the entire file of the procedure should be shared with all parties to the complaint procedure.	
Vote of the members of the EDPB The votes of the members of the EDPB are kept secret and the EDPB does not publish the details of the votes by each member. It is therefore not possible to verify that the relevant procedure to adopt a decision has been followed by the members and makes it impossible to challenge before the CJEU.	The vote of the members of the EDPB on an Article 65 GDPR procedure should be made public or at least shared with the parties to the complaint procedure to enable them to verify that the decision-making procedure meets the requirements of Article 65 GDPR.	
Notification that a decision under the consistency mechanism has been submitted to the EDPB According to Article 57(1)(f) and Article 77(2) GDPR, the complainant must be informed of every step of the procedure. In one particular case, the Irish SA informed the complainant that they would not be	It should be made explicitly clear that the complainant should be informed in all cases that their complaint is sent to the EDPB. They should be informed on the date, the timeline envisaged, and how their procedural rights will be respected in terms of right to be heard and to access the file.	

informed about the sending of the case to the EDPB.[15]		
Right for the complainant to trigger Article 65(1)(b) GDPR In some cases where the SAs take longer than a "reasonable time" to determine which SA is the LSA, the complainant should be able to ask for a binding decision from the EDPB under Article 65(1)(b) GDPR.	EDPB should adopt its Rules of Procedure to provide such possibility for the complainant to ask for a binding decision.	See cases C014 and C026 mentioned above.
Topic 5 – FINAL DECISION		
The complainant is not always notified of the decision Sometimes the complainants are not informed about the issuance of a decision, especially in the one stop shop mechanism. Under Article 60(8) GDPR, the SA receiving the complaint should issue a decision on the complaint when the complaint is dismissed or rejected. The SA should communicate the full decision of the LSA to the complainant and not be the only one deciding whether the complaint has been rejected or dismissed. It is up to the complainant to assess this element and decide to appeal the decision or not. This can only be done if the complainant also received the decision from the LSA.	There should be an explicit obligation to notify the complainant when a decision has been taken, and to send a copy of the full decision. There should be an obligation to mention the status of the decision/document (final, mere advice, draft, or other), that an appeal is possible and what the deadline to appeal is (see below). Also in cross-border cases, the decision issued by the LSA (and not just a summary thereof) should be communicated to the complainant.	See the complaint filed by La Quadrature du Net against Amazon, where the Quadrature was just informed by the French SA about the existence of the decision adopted by the LUX SA and shared a summary of it. See https://www.laquadrature.net/wp-content/uploads/sites/8/2021/08/CNIL_CLP211124.pdf In one of *noyb*'s 101 complaints on EU-US data transfers, *noyb* only learned about a decision by the Italian SA because of media coverage. The SA did not inform *noyb* of the decision and only provided it on request.
Unclear if a decision was issued – no decision It is sometimes not clear to the complainant whether the answer given by the SA is a decision, or another outcome.	There should be an obligation to issue a clear final decision. If the decision/document is not final, the SA should explain what the future steps are and when a final decision will be issued.	See answer from the LUX SA after a complaint filed against Apollo and Rocketreach, challenged by *noyb:* https://noyb.eu/en/luxemburgs-watchdog-refuses-show-its-teeth-us-companies

[15] See, for example, the letter from the Irish SA to *noyb* in the complaint against Instagram before the Belgian SA, where the Irish SA writes that *"Please note that, if no (or no suitable) proposals are submitted to this office prior to the specified deadline, the DPC will proceed to refer the Objections to the EDPB for determination pursuant to the Article 65 GDPR dispute resolution procedure without further notice to you."*

Since the status of the document sent by the SA (decision to reject or to enforce, advice, or update) determines whether an appeal is possible or if the complainant should wait for a final decision, it is necessary for the SA to mention what type of document is issued to avoid confusion.	Especially the rejection of a complaint must be a formal decision subject to appeal. The reasons for the rejection must be mentioned in the decision and be subject to judicial review.	
Violation found, no action taken Some SAs confirm that a violation takes place but still do not take any action.[16]	SA finding a violation that still exists at the time of the finding should always take action to enforce the GDPR and order the controller to end the violation.	
Language of decisions Sometimes the language of the decision is different from the language of the complaint (both official languages of a Member State, like in Belgium for example).	SAs should stick to the language chosen by the complainant, while respecting further requirements imposed by national rules. If there are several official languages in a Member State, the complaint defines the language of the procedure, without prejudice to the translation of the document for the controllers, if necessary.	*noyb*'s 101 complaints lodged in Luxembourg: Complaints in German, decision in French. Complaints in Belgium against Instagram.
Publication of the decisions The SAs have different approaches regarding the publication of their decisions. - Some SAs publish as a general rule every outcome of a complaint (like the Belgian SA), including the rejection of the complaint. - Some SAs seem to publish some decisions on a case-by-case basis without a consistent approach (like the EDPS). - Some SAs redact the names of the controllers whereas some decide on a case-by case basis. - Some identify controllers only as additional sanction, and may have	All SAs should publish any outcome of all cases (complaint or *ex officio* investigation, sanction or dismissal of the case) on their website. The names of the parties should only be redacted where appropriate and in limited circumstances.	

[16] For example, the Irish SA recently wrote a letter to a complainant confirming that their right to access was indeed violated but it rather invited the complainant to go to court instead of enforcing a decision against the controller.

limitations linked to the time of the identification of the sanctioned controller (e. g. the CNIL). - Some SAs refuse to publish or even to share the final decision with the complainant (like the Lux SA in the case of Amazon). This **limitation of access to the decisions** of the SAs makes it difficult for the complainants, the controllers, processors, academia and the civil society to follow the actions of the SAs, to understand the underlying legal motivation of their decisions and therefore to access knowledge and guidance about how to comply with the GDPR. It also negatively impacts the accountability of SAs. The systematic **redaction of the name of the parties** does not make much sense: transparency of the action of the SAs and controllers should be the rule, whereas confidentiality should only apply in certain specific cases.		