General topic	Description of a specific problem under the general topic	Ideal solution	Article(s) involved (national, EU, or other)	Reference to specific noyb cases	References to EDPB documents / table	Comments	Proposed Solution
I. Filing a complaint							
Admissibility - Formal requirements: signature	In some Member States, an electronic mail is enough for validly filing a complaint with a supervisory authority (SA), while in others, the lack of a written signature on paper leads to inadmissibility of the complaint.	The procedural provision should mention the minimum formal conditions for filing a complaint with a SA. When met, the complaint should always be deemed admissible.	Article 77 GDPR		EDPB Letter to the EU Commission on procedural aspects that could be harmonised at EU level ("EDPB wish list") : FN 16, referring to EDPB coptribution to the evaluation of the GDPR, page 10: national legislation in AT, BE, BG, IT, LV, NL, PL, SI, ES foresees formal admissibility requirements. On the other hand, no admissibility requirements are foreseen in CZ, DK, DE, whereas a discretionary power regarding the assessment of admissibility is exercised in LU.		**Concept 2** would ensure that the national law of the filing SA is relevant for any rules on the admissability of the law and other SAs may not review the admissability.
Admissibility - Formal requirements: proof that the not-for-profit entity is certified	Some SAs request additional documentation with regard to the representation of data subjects by not-for-profit organisations under Art. 80(1) GDPR. Not only a representation agreement is requested to be filed in the country's official language but also a proof that the specific organisation is allowed to represent data subjects.	The procedural provision should mention the minimum formal conditions for the representation of data subjects. When met, the complaint should always be deemed admissible.	Article 80(1) GDPR	Poland in all C-037-... cases ("cookie banners") where the Polish DPA required addition proof or representation. See also Bulgaria asking, 2 years after the complaint, to have a representation agreement in Bulgarian signed before a public notary.			**Concept 2** would ensure that the national law of the filing SA is relevant for any rules on the admissability of the law and other SAs may not review the admissability.
Admissibility - Substantive requirement: residency of the complainant or other link with the territory of the SA	In some Member States, complaints are considered inadmissible if the complainant is not a resident in the Member State of the SA. Article 77 provides that data subjects have the right to lodge a complaint with a SA "in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement (...)". The words 'in particular' leaves room for interpretation and legal uncertainty.	A complaint should always be deemed admissible by the SA of a Member State *at least* on the basis of the complainant's residence or place of work, or on the basis of the place where the infringement occurred, with the possibility for SAs to also accept complaints based on any other relevant circumstances.	Article 77, 80 GDPR		See internal EDPB document 6/2020 on preliminary steps to handle a complaint: admissibility and vetting of complaints		The matter is already clear from the wording of the GDPR, but could be mentioned in recitals and futrther specified in the procedural regulation.
Admissibility - Substantive requirement: prior request to the controller	Some SAs reject complaints where the data subject has not made a prior request to the controller in the context of the exercise of his or her rights under Article 15 to 22 of the GDPR. As a result, in some Member States, complaints are only admissible after (1) the data subject has provided a written request to the controller and (2) the 1-month period foreseen under Article 12(3) GDPR for the controller to answer has passed. When the issue is precisely that the data subject cannot identify the controller or contact the latter because of a lack of information, the SA should not be able to reject a complaint on the basis that a prior request has not been made.	Article 77 GDPR should clarify that the exercise by the data subjects of one of their rights under Article 15 to 22 is not a prerequisite for filing a complaint with an SA, or should clarify if and in which cases such a prior request must be made.	Article 77, 80 GDPR	Spanish Supreme Court n° 1039/2022 (https://gdprhub.eu/index.php?title=TS_-_1039/2022).	EDPB document 6/2000		The GDPR does not seem to require an attempt to agree with a controller, but **Concept 2** would allow to ensure that the national law of the filing SA is relevant for any rules on the admissability of the law and other SAs may not review the admissability, including such pre-conditions.
Admissibility - Substantive requirement: identification of relevant legal grounds	Some SAs refuse a complaint if the legal grounds for such a complaint are not identified.	The provisions should prohibit to ask to specify legal grounds as the complainant might not be in a position to identify them and does not have the legal expertise to do so.	Article 77, 80 GDPR		see EDPB internal document 6/2000 and EDPB internal document 02/2021 (§57) (cf. the notion of 'substantiated complaint' should form a less higher threshold than some SAs expect from complainants.		The formal threshold is not defined in the GDPR. It seems that Concept 2 ensure that the national law of the filing SA is relevant for any rules on the admissability of the law and other SAs may not review the admissability and require such additional elements.
Admissibility - Formal requirement: e-gov solution	Some SAs refuse complaints that are not filed via a national e-Gov access system or solution, whereas the complainant might not have the possibility to do so (e.g. because she or he is not a resident or because an organisation is filing under Article 80 GDPR).	The new text should oblige SAs to accept complaints without requiring the use of any e-gov access system. Or, as a minimum, the e-gov solutions from other Member States should be accepted throughout the EU (see also eIDAS).	Article 77 GDPR	Spanish and Polish cases where the SA is asking to use the national e-access.	EDPB wishlist, page 7		**Concept 2** would allow to ensure that the national law of the filing SA is relevant for any rules on the admissability of the law and other SAs may not review the admissability.
Admissibility - Limitation period	Some complaints are rejected because of a limitation period / statute of limitation. For example, a time limit for introducing the complaint is envisaged in AT and SK law.	The matter should be harmonised (e.g. one year as from the day the data subject became aware of the violation).	Article 77		EDPB wishlist, page 7		**Concept 2** would allow to ensure that the national law of the filing SA is relevant for any rules on the admissability of the law and other SAs may not review the admissability.
Contradictory decisions on admissibility	Once the CSA have assessed the admissibility of a complaint, some LSAs make a contradictory assessment and reject the complaint.	The provision should specify that a LSA cannot consider inadmissible a complaint that has already been recognised admissible in another Member State by a CSA.	Article 78(2) and 79(2) GDPR		The EDPB internal document 06/2020 clearly states that "*the complaint has to fulfil formal conditions of the MS where it was lodged. Thus, if deemed admissible there, the LSA shall not re-examine the admissibility of the complaint* " and cannot reject it. See para. 16-17.		**Concept 2** would allow to ensure that the national law of the filing SA is relevant for any rules on the admissability of the law and other SAs may not review the admissability a second time.
Competence of the SA - GDPR vs ePrivacy	If a complaint is filed both under the GDPR and the national ePrivacy Law, it is not clear how the different authorities (if they are different) deal with the complaint, who is competent, etc.	The matter should be harmonised, stating that both authority can deal with the complaint at the same time, or in cooperation, without obligation to wait for the other authority to deal with the case.	Art. 77 GDPR, national ePrivacy Law	Some C-037-... cases ("cookie banners") in Ireland, Norway for example			**Concept 2** would ensure that the national law of the filing SA is relevant for any rules on the admissability of the law. If an SA only has jurisdiction on GDPR, it can reject the ePrivacy element or forward it to the relevant regulator - as forseen in the national law.

General topic	Description of a specific problem under the general topic	Ideal solution	Article(s) involved (national, EU, or other)	Reference to specific noyb cases	References to EDPB documents / table	Comments	Proposed Solution
II. Information on the status of the complaints							
Effective procedure - transparency : information on the status of the complaint	Article 78(2) GDPR provides that SAs must inform the data subject "*within three months* " on the progress or outcome of the complaint. Often, data subjects do not get any update at all, or only after several months / years, despite asking for such information and sending reminders. The EDPB position according to which it would suffice for SAs to give one single update within three months after the complaint has been filed does not make any sense, since it would allow SAs to simply acknowledge receipt of the complaint and then leave the data subjects in the dark.	The text should state that information on the status and progress of the complaint should be provided by the responsible SA to the complainant every 3 month as from the date of the filing, and specify what this update must at least contain (see below).	Articles 77 and 78 GDPR			In all the cases we handle, only a few authorities frequently inform the complainant on the status without the complainant repeatedly asking for an update. In cooperation cases, usually neither the CSA nor the LSA provide any updates. Asking the CSA leads to the CSA asking the LSA for an update and - if the complainant is lucky - giving the complainant an update months after the complainant's request (if at all). Asking the LSA directly for an update may lead to a quicker update, but often the LSA refers the complainant back to the CSA for updates (see noyb cases C007 and C008, email dated 27.11.2020) or they are even unable to identify the case (happened in various cases of the 101 complaints). The Polish SA responds very randomly to requests for updates sent to them via the eGov system. Sometimes they respond within days, but sometimes they are silent for months. This is the case in all cookie banners complaints filed in Poland and in C029-101, C029-26, C029-27, C029-28, C029-29 ("101 complaints").	**Concepts 2, 7, 8, 9 and 14** could ensure that the CSA has full access to the case file at any time, give updates and that LSAs have clear deadlines to follow.
Effective procedure - transparency : SA in charge of informing complainant	It is unclear which SA is required to provide information to the complainant regarding the progress of the procedure, since 60(7) and Article 77(2) requires the SA "*with which the complaint has been lodged* " to provide such information while Article 78(2) refers to the SA "*which is competent pursuant to Articles 55 and 56* " (the CSA or LSA).	The procedural text should specify that the SA in charge of informing the complainant is the one that is *de facto* handling the complaint at the time (i.e. first the SA where the complaint was lodged, then the LSA once the complaint has been transferred, and finally the original SA again in the event the LSA rejects/dismisses the transferred complaint).	Article 60(7), and Articles 77 and 78 GDPR	Complaint with the Be SA against Instagram: the update is sometimes coming from the BE SA, sometimes fromt the Irish SA.			**Concepts 2 and 7** (joint case file) could ensure that the CSA can give these updates instantly.
Effective procedure - transparency : content of the information to complainants	Sometimes the update is not substantial enough for the complainant to understand what has been done or still needs to be done.	The information shared with the complainants should be substantial, and mention at least (1) the status of admissibility of the complaint; (2) the actions that have already been undertaken by the SA/LSA and the next envisaged steps; (3) whether they intend to start an investigation, and if no, why not (4) the expected timeline for a decision, (5) the reasons for any delay, and (6) the possibility for the complainants to share their views.	Article 77			noyb's 101 complaints are a good example: The replies received by the Austrian SA (as CSA) when asking for an update is usually a standard reply along the lines of "complaint continues to be under investigation... coordination with LSA ..." without any report on what has happened so far. In Luxembourg, never has anything substantial to report, other than the fact that the Luxembourgish SA had declared themselves to act as LSA. When asking the Luxembourgish SA for an update, the only replies are boilerplate responses along the lines of "complaint continues to be under investigation". C016 has been pending for 3 years and 9 months and we know virtually nothing about it's progress. C040 has been pending for 1 year, with no information whatsoever. The same concerns cookie banners complaints. The AT and most German SAs (with the exception of Berlin, maybe) give very scarce short "updates" that they are still investigating. The PL SA likes to send very long formal letters with lots of text but they do not provide an substantial information apart from "we are investigating the issue".	This matter is **not** included in any *noyb* concept, but should be included in a Regulation, when defining these updates.
III. Holding SAs accountable in case of inaction							
Remedy against the competent SA for not informing the complainant regularly	Article 78(2) is not clear about what can be expected as a judicial remedy when the SA (or the CSA/LSA in the context of the OSS mechanism) is not properly informing the complainant about the course of the procedure. 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 no procedural step has (yet) be taken since the last update communicated to the complainant. 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.	The provision should specify what can be asked to the court in the event a data subject is not being updated every three months, e.g. forcing the SA to provide regular substantial updates, and to explain reasons for not providing these updates on time.	Articles 77 and 78 GDPR	In a complaint 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.			**Concepts 2, 9 and 14** should limit the need for updates, as the cases should be decided within a reasonable timeline. Updates themselves that only say that the case is under investigation do not seem overly useful. **Concpet 5** (the EDPB subbody) could be used to enforce requests between SAs.

General topic	Description of a specific problem under the general topic	Ideal solution	Article(s) involved (national, EU, or other)	Reference to specific noyb cases	References to EDPB documents / table	Comments	Proposed Solution
Remedy against an SA for not handling complaints within a reasonable period	Article 78(2) GDPR provides that data subjects have the right to an effective remedy against the SA when the latter does not "handle" the complaint. Because the term "handle" is undefined, and because no clear procedural deadlines exist, it is difficult to understand when the data subject could have a claim against an SA when a complaint is not handled within a reasonable period. If clear deadlines were set for the SA to issue (1) a decision on admissibility and (2) a final decision, it would be easier for data subjects to hold their SA accountable for delays.	SAs should be subject to clearer deadlines (see below, section V on procedural deadlines), so that data subjects can hold them accountable for lack of actions. The provision should also specify what can be asked to the court in the event an SA does not meet the applicable deadlines, e.g. forcing the SA to issue a decision. The provision could also specify that a breach of procedural deadlines gives rise to damages.	Articles 77 and 78 GDPR				**Concepts 9 and 14** should properly define the complaint procedure and deadlines. Concept 5 should be sufficient to ensure that LSAs comply with their duties.
Remedy against SA for not handling complaints with due care	SAs sometimes render a decision by which they close a case because they were unable to identify or contact the controller, or because they could not find any evidence of a violation. In some other cases, SAs do find a violation but do not adopt any corrective measures (e.g. injunctions). In other words, even when a complaint is being handled, the concrete actions of SAs are sometimes very disappointing (i.e. no use of their investigative or corrective powers, although this would be necessary to establish the existence of a violation and/or put an end to it).	SAs should be subject to an obligation of due care, according to which they should justify why they did not use their investigative or corrective powers. The provision should also specify what can be asked to the court in the event an SA wrongfully decided not to use its investigative or corrective powers, in breach of its obligation of due care, e.g. forcing the SA to take action, to open an investigation, to issue an injunction, etc. The provision should also specify that a breach of the due care obligation gives rise to damages.	Articles 77 and 78 GDPR			To be appreciated together with the discretionary powers of administrative bodies.	**Concepts 9 and 14** should properly define the complaints procedure and deadlines. Concept 5 shoudl be sufficient to ensure that LSAs comply with their duties.
Remedy against CSA/LSA in the context of the OSS	Same as above in the context of the OSS.	The text should be specify that, in the context of the OSS mechanism, the right to an effective against an the concerned SAs should entail: - a positive duty to cooperate and a duty of the CSA to engage with the LSA in the case of inactivity; - the possibility to ask the court 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, etc); - 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.	Articles 77 and 78 GDPR	Complaints against Instagram, Facebook and WhatsApp in Belgium, Austria and Germany, where the filing SAs refused to broaden the scope of the investigation conducted by the DPC, despite the numerous requests from noyb, and the EDPB decision after 5 years to side with noyb and force the DPC to investigate further. However, a large number of the points of the complaints remain not addressed after 5 years and noyb is struggling to force any of the SAs involved to investigate the complaint. Besides, the different SAs where the complaint was filed just informed noyb that the Irish SA issued a decision, under Article 60(7), which implies that the complaint was upheld, whereas the decision of the Irish SA does not adress all points of the complaint, and is therefore a partial rejection, which should lead to a decision by the BE, DE and AT SAs under Article 60(8) GDPR. This (negative) decisions can be challenged before their respective national courts. The possibility to challenge the decision of the SA where the complaint is filed is therefore depending on the SA itself, which can wrongly qualify the decision and instead, simply inform the complainant. This "information" is not a "decision",		To be appreciated together with the discretionary powers of administrative bodies.	**Concept 5** shoudl be sufficient to ensure that LSAs comply with their duties. Additional clarifications on the remedy under Article 78 GDPR shoudl be added.
IV. Obligation to issue a formal decision or reach an amicable settlement							
Procedural rights - obligation for SAs to issue legally attackable decisions	Some SAs take the view that "handling a complaint" in the sense of Article 57(1)(f) GDPR includes closing a case without any investigation, without giving any reason, and without issuing any legally attackable decision on the matter. As a result, SAs are sometimes rejecting, dismissing or closing a complaint (e.g. because they consider that they are not competent, that the complaint is frivolous or that some formal/substantive requirements are not met (cf. admissibility)), without adopting a formal administrative act that is legally attackable. 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 of the case, and not when the SA remains inactive. That is because the term "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 specify that "handling a complaint" (in Article 57(1)(f) GDPR) means looking into the complaint and issuing a formal decision. In other words, all complaints must lead to a legally attackable decision, even if that decision is about rejecting/dismissing a complaint, and that such a decision can be appealed as per Article 78(1) GDPR. The only exception to this obligation would be in cases where the complainant decides to voluntarily withdraw his or her complaint.	Article 57(1)(f) GDPR and 78(1) and (2) GDPR	The LUX SA, in the Apollo and Rocketreach case, sent a letter to the complainant saying that the controllers was based outside of the EU and therefore cannot reach them. The status of this letter is unknown and is now subject to appeal before the Court	EDPB internal document 02/2021 which provides a definition of the term 'handle' in para. 61.	FM: National administrative law in most Member States could be of inspiration, as (i) appeals against inactivity are mostly provided for and (ii) there is a duty to justify administrative decisions in almost all cases.	**Concepts 11 and 12** would largely solve these issues.

General topic	Description of a specific problem under the general topic	Ideal solution	Article(s) involved (national, EU, or other)	Reference to specific noyb cases	References to EDPB documents / table	Comments	Proposed Solution
Procedural rights - SAs switching to an ex officio procedure	Some SAs are inclined to suspend or put an end to a complaint procedure and simultaneously open an ex officio procedure aimed at resolving broader compliance issue with a specific controller. This deprives the complainant from his/her other procedural rights, including the right to be informed about the status of the case, or to appeal the decision taken by an SA.	The text should made clear that all complaints should be followed by a formal decision, even when a complaint triggers a parallel ex officio procedure. The proposed draft regulation should ban the practice whereby the opening of an ex officio procedure suspends or puts an end to a complaint procedure, or at least foresee a mechanism by which the start of an ex officio procedure does not frustrate the very purpose of a complaint procedure, i.e. obtaining a "legally attackable act".		See for instance, noyb C015 against Spotify (cf. IMY structurally turns complaint procedures into ex officio ones). Similar situation in Ireland.	Internal EDPB Document 02/2021 on SAs duties in relation to alleged GDPR infringements, p. 10).		**Concepts 9 and 10** would largely solve these issues.
Procedural rights - effects of amicable settlements on the rights of the complainants	Recital 131 GDPR mentions the possibility for SAs to reach an amicable settlement ; some SAs (and the Irish SA in particular) systematically uses this to "handle" complaints. Once a complaint has been 'settled', the complaint is considered as closed or withdrawn. This can have an adverse effect on the procedural rights of the data subjects.	The text should provide a legal basis and harmonise the definition, the conditions and the procedural elements for the amicable resolution of complaints: - definition: an amicable settlement should be defined as a process where the controller/processor and the complainant reach an amicable solution, and where the SAs act as a mediator; - legal basis: the text of the GDPR itself should provide the legal basis for amicable settlements. ; - conditions: the text should clarify when and how amicable settlements can take place (e.g. upon proposition of the data subject, the controller, and/or the SA), as well as a maximum timeframe for the negotiations. In no circumstances should the amicable settlement be possible without the prior agreement of the complainant (otherwise, amicable settlement can become an exit door for controllers).	Recital 131 GDPR	See cookie banners cases: 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	Inspiration can be drawn from EDPB internal document 06/2021 on amicable settlements.	For the Irish DPC, trying to reach an amicable settlement first is the default mode of action. With regard to the process for the handling of complaints, Section 109(2) of the Irish Data Protection Act 2018 provides that the DPC, 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. The DPC has therefore taken an approach that it "must first examine the possibility of arranging an amicable resolution of complaints". In situations where complaints are amicably resolved, they are deemed to have been withdrawn by the complainant.	**Concepts 9 and 14** should take care of these issues. A general definition of "amicable resolutions", highlighting that they must be based on a withdrawl of the complaint by the data subject and must be somewhat formal would be useful.
Effective procedure - amicable settlements in the context of the OSS	Having recourse to an amicable settlement should not interfere with the prerogatives of the CSA/LSA in the context of cross-border cases.	The text should put the CSA/LSA under the obligation to follow the cooperation procedure in case of cross border cases, even if an amicable settlement is found. If the CSA suggests an amicable settlement, the LSA should be involved in the process as well. Conversely, if a CSA suggests an amicable settlement, it should inform the LSA. Amicable settlements should remain legally challeangeable acts in the case where the right of the data subject, the controller or the prerogatives of the CSA/LSA have been infringed. The amicale settlement should in any case be considered as a decision, subject to judicial challenge and one-stop-shop procedure.			EDPB internal document 06/2021, para. 37-38. "the LSA is required to submit the draft decision setting out the terms of the settlement to the CSAs in accordance with Article 60", this is a sui generis decision finding that the complaint is settled. Internal document lists the information that the draft decision should entail, see para. 57.		**Concepts 9 and 14** should take care of these issues. A general definition of "amicable resolutions", highlighting that they must be based on a withdrawl of the complaint by the data subject and must be somewhat formal would be useful.

General topic	Description of a specific problem under the general topic	Ideal solution	Article(s) involved (national, EU, or other)	Reference to specific noyb cases	References to EDPB documents / table	Comments	Proposed Solution
Procedural rights - 'letter' instead of a decision	Some SAs issue advices or informative letters on the outcome of a complaint instead of a decision. The status of such letters is unclear.	The procedural regulation should include formal requirement relating to the outcome of a complaint: they should always be decisions (e.g. the decision should be rendered in writing and be dated + the decision should include a statement according to which the complainant has the right to challenge that decision pursuant to Article 78(1) GDPR within the applicable deadline).		For example, a member reported a case where the Irish SA provided an "advice" to the complainant under Section 109(4) of the Irish Data Protection Act, instead of issuing a formal (and thus legally attackable) decision.	EDPB internal document 02/2021 , see para. 61 and further.		**Concept 11** should ensure that there is minimal requirements for "decisions".
V. Lack of procedural deadlines							
Effective procedure - no deadline for deciding on the admissibility of a complaint	Some SAs do not confirm within a reasonable time whether the complaint filed by an not-for-profit organisation under Article 80 GDPR is admissible. For example, some SAs inform the complainant/his or her representative more than one year after the complaint has been filed that (i) some formal or substantial requirements are not met, (ii) that the alleged violation has stopped, (iii) that the representation agreement is not valid or (iv) that they do not consider themselves competent.	The drat regulation should specify that the SA should immediatelyacknowledge receipt of the complaint, and must render a decision on the admissibility of the complaint within a period of maximum 3 months.	Article 77, 80 GDPR	Case Apollo and Rocket Reach: the Lux SA has questioned the right of noyb to represent the complainant and file an appeal before the court. See also 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. The Polish SA in the cookie banners complaints reacted to the first batch of the complaints (Aug 2021) within two weeks and has not reacted at all to the second batch (Aug 2022) yet (over two months down the line). The IT SA has not confirmed the receipt of the cookie banners complaints at all yet (over 1 year). The other SAs, such as e.g. Norway, Belgium take a random amount of time (usually a few months) to confirm the admission of complaints ("cookie banners" project).			**Concepts 9, 10, 14 and 16** should solve these issues.
Effective procedure - competence of the SA	The absence of deadline regarding whether a SA considers itself competent delays the procedure (by contrast, Article 56(3) GDPR provides that when a case is transferred by an SA to a LSA, the latter has 3 weeks to confirm whether it will handle the case).	The text should provide such a deadline. The decision whether or not a SA considers itself competent should be subject to a deadline, i.e. within 3 months from the day of receipt of the complaint.		See google case from noyb at the CNIL which took more than 4 years to reach a conclusion on the LSA. The decision is not reached yet.			**Concepts 9, 10, 14 and 16** should solve these issues.
Effective procedure - OSS - no deadline to transfer a complaint to the LSA	The lack of deadline for an SA to transfer the complaint to the LSA is slowing down the procedure.	The text should provide for such a deadline. The decision whether or not to transfer a case to the LSA should be taken together with the decision on the admissibility of the complaint and the competence of the SA, i.e. within 3 months from the day of receipt of the complaint.	Article 56(3) GDPR	See AT case against Netflix where the SA did not send the procedure to the LSA for 2 years.			**Concepts 9, 10, 14 and 16** should solve these issues.
Effective procedure - start and duration of an investigation	The absence of any deadline regarding the start and length of an investigation may substantially delay the procedure.	The text should provide for such a deadline (with possible extensions, depending on the complexity of the case).					**Concepts 9, 10, 14 and 16** should solve these issues.
Effective procedure - OSS - no deadline for draft decision of LSA (or revised draft decision)	The absence of any deadline for the LSA to prepare a (revised) draft decision to the CSAs delays the entire procedure.	The text should provide such a deadline.	article 60(3) +60(5) GDPR				**Concepts 9, 10, 14 and 16** should solve these issues.
Effective procedure - OSS - no deadline for final decision of LSA	The absence of any deadline for the LSA to issue a final decision the entire procedure.	The text should provide such a deadline.	Article 60 GDPR				**Concepts 9, 10, 14 and 16** should solve these issues.

General topic	Description of a specific problem under the general topic	Ideal solution	Article(s) involved (national, EU, or other)	Reference to specific noyb cases	References to EDPB documents / table	Comments	Proposed Solution
Effective procedure - OSS - no deadline for triggering Article 65 procedure	There is no deadline to trigger an Article 65 procedure if no consensus can be reached.	The text should provide such a deadline.	Article 60(4) + 65 GDPR	See Irish cases against Meta where the DPC waited without reason before sending the case to the EDPB. See also CNIL case against Google where the CNIL and DPC waited before asking the EDPB to take a position on who is the competent authority, and then withdrew their application to the EDPB. The case is still pending and noyb is still waiting to be informed about who is the competent authority.			**Concepts 9, 10, 14 and 16** should solve these issues.
Effective procedure - OSS -deadline for the consistency procedure	There is currently no deadline to start an Article 65 procedure once the file has been sent to the EDPB.	The procedural regulation should override the EDPB Rules of Procedure and state a clear deadline for the EDPB to start the consistency procedure under article 65	Article 65 + Rules of Procedure EDPB	See example of Google complaint above.			**Concepts 9, 10, 14 and 16** should solve these issues.
Effective procedure - OSS - deadline for sharing files with complainant	There is currently no deadline for the CSA to forward the submissions or other exchanges files of the case from the LSA to the complainant.	The text should provide such a deadline.		See Grindr C-012 case. It took 6-7 months for the SAs to deliver the controller's submission to the complainant.			**Concepts 7, 9, 10, 14 and 16** should solve these issues.
VI. Access to file and right to be heard							
Procedural rights - Status of the parties to the procedure	Complaint procedures generally involve the intervention of the following actors: - the data subject(s) / complainant(s) - the representative of the data subject(s) (if any) - the controller or processor (if identified) - the SA (or CSAs and LSA). There is currently no indication in the GDPR with respect to the status of these different actors, and whether in particular the complainant should be considered as a party to a complaint procedure. The lack of harmonisation makes the exercise of procedural rights particularly challenging in the context of cross-border cases.	The text should clarify who ought to be considered a party to the procedure, the rights/obligations attached to this qualification and the legal basis for it. Procedural rights for each party should at least include: - the right to access all documents of the file; - the right to be heard, including the right to submit one's factual and legal arguments throughout the procedure; - the right to appeal any decision rendered by the SA. In cross-border cases, some procedural rights are provided by one SA but not by the LSA or the EDPB (or conversely).		See Swedish case on Spotify, where noyb was denied to be a party to the procedure and could allegedly not go to court. This was then overruled by the Swedish courts.	EDPB internal document 02/2021 states that Article 77 does not establish a right for a complainant to become a party to the procedure, see para. 44. The Contribution of the EDPB to the evaluation of the GDPR under Article 97 confirms, on page 11, that the complainant is "not being always perceived as a party to the proceeding before the SA". This is also shown by the "*Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities* " issued by the EDPB on 5 August 2021. By way of example, according to this report, complainants have a right to be heard under Austrian, Belgian, Bulgarian, Irish, Maltese, Norwegian and Polish law; by contrast, this is not the case under Czech, French, and Swedish law. Under Spanish law, complainants are not considered as parties except where the envisaged decision may adversely affect them which is assessed on a case-by-case basis but is by default deemed to be the case in all proceedings related to the exercise of data protection rights		**Concept 9** should take care of this matter, as well as proper definitions in the Regulation.
Procedural rights - Access to the file: scope of the right to access and restrictions	Member States have divergent approaches in terms of granting access to (procedural) documents to the parties. For exmaple, some SAs unilaterally decide that some documents or parts of documents should be confidential, sometimes without any clear legal basis. Some SAs also bar access to the file by arguing that the complainant cannot be considered a party to the procedure (including in the event of ex officio procedures initiated on the basis of a complaint).	The text should harmonise the rules concerning access to the file in the various stages of the procedure before the national SA, the CSA, the LSA, and the EDPB. As a general rule, the complainant should be able to access all documents to rebut the submissions of the controllers and processors, or the opinions of the SAs. Exceptions to this general rule can exist when the file contains confidential information but should be interpreted restrictively, in light of the right to access and the right to be heard of the parties. The text should clearly define these exceptions. Also, rather than not communicating the file at all because of the confidential nature of some information, the SAs should provide at least a redacted copy excluding such confidential information (e.g; trade secrets, IP-protected material, personal data, etc).		See also some SAs (like the CNIL) where the complainant is not even involved int he procedure (no right to be heard, no access to the file). At the opposite, the BE SA is granting full rights (except, it seems, in cross-border cases , like Instagram, where the BE SA refused to give access to the file, follwing the rules of the Irish SA).			**Concept 2** should take care of this matter, as the national law of the relevant CSA/LSA applies, but the minimum guarantees of Article 41 CFR has to
Procedural rights - Access to the file: modalities of access	SAs do not always provide electronic access to documents, but require the complainant to make a written request or to come in-person to have access to the file. Also, some SAs make the access to the file dependent on the signature of an NDA (e.g. the Irish SA). Modalities to access the file should not unduly restrict such access.	The text should provide that the access to the file should be permitted electronically, and that this access should not be subject to additional formal or substantive conditions or restrictions, such as signing an NDA.		noyb cases C029-101; C029-26; C029-27; C029-28: the Polish SA refused the request to access the files electronically *despite* a novelisation of the Code of Administrative Procedure that permits the SA to do that. The SA's justification was that the case has gathered over 500 pages of files (on paper) and they have limited human resources and a limited number of scanners in the office so it would have taken them too long to scan all the files. noyb case against Meta: the Irish SA requested that noyb signs an NDA to have access to documents in the file.	see EDPB wish list documnt referring to the access to the file in Poland which is only possible upon an in-person appointment (see footnote 4)		**Concepts 2** (applicable law) **and 7** (joint file) should take care of the matter.

General topic	Description of a specific problem under the general topic	Ideal solution	Article(s) involved (national, EU, or other)	Reference to specific noyb cases	References to EDPB documents / table	Comments	Proposed Solution
Procedural rights - Right to be heard	Some SAs only allow submission on the "facts" from the complainant, but not on legal arguments.	The text should male clear that the right to be heard of the complainant includes the right to share submissions on the law and the facts in response to the controller's submissions or the SAs' (draft) opinion.		See noyb case C-037-10095: the German SA refused to hear the legal arguments of the complainant.			**Concept 2** (applicable law and "leveling up") should take care of the matter.
Procedural rights - Language of the procedure	Sometimes the language of the procedural documents (e.g. investigation reports ; submissions by the controller; etc.) is different from the language of the complaint (including in Member States with multiple official languages, like in Belgium for example). In the context of the OSS mechanism, 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 the complaint/ procedure.	The language of the complaint should define the language of the procedure before the CSA, without prejudice to the translation of the document for the controllers, if necessary. In the context of the OSS mechanism, the SAs should translate the documents into the original language of the procedure or the preferred language of the complainant before providing these documents.		See e.g. Belgian SA sending documents to noyb in English, despite English not being a national language. Equally, the Austrian SA sends autotranslated documents, that are sometimes of such poor quality that the arguments of the opposing side cannot be understood.			**Concept 2 and 7** shoud address these issues.
VII. Cooperation procedure							
Procedural right - challenging the decision designating a LSA	It is currently difficult for the controllers, the complainants or their representative to contest the decision of a SA designating a LSA, since this type of decision is usually not shared with the parties.	As already pointed out above (Section V. Procedural deadlines), the SA should be obliged to issue a decision on (1) the admissibility of the complaint ; (2) its competence as LSA and/or (3) the decision to transfer the complaint to a LSA within three months from the day of the receipt of the complaint. This decision should be subject to judicial challenge. If the decision designating the LSA is being challenged, the EDPB should be responsible for determining who that LSA is on the basis of Article 65(1)(b) GDPR. The complainant or the controllers should be able to trigger Article 65(1)(b) GDPR, as not obstacle to this course of action exists in the GDPR. Furthermore, procedural law should also deal with how to assess the evidence on where the main establishment is located.	Article 56 GDPR	1) noyb case on forced consent by Google: 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. The case was then withdrawn by the CNIL for reasons not shared with *noyb,* left in the dark. 2) noyb case C014: 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 SA 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. 3) noyb case C026: the situation here is similar to the one mentioned 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	The EDPB guidelines on LSA say is that SAs should cooperate to assess this, and should not solely base their statements upon statements provided by the controller or processor.		**Concepts 3 and 5** address this issue.
Effective procedure - challenging the scope of the investigation as determined by the LSA	Many responsibilities rest upon the LSA in the context of the OSS mechanism, and in particular deciding on the scope of the investigation itself (i.e. which potential breaches are being investigated). Later in the procedure, the CSAs can only share their reasoned objections on the draft decision communicated by the LSA within that scope. It is too late to ask the LSA to extend the scope of the investigation to other potential breaches. Some SAs are even not allowed due to their national procedural laws to extend the scope of their investigation after a draft decision is shared (see e.g., Belgium).	Before submitting a draft decision on the merits of the complaint, the LSA should first consult and agree with CSAs on the scope of the investigation itself.	Article 60(3) GDPR	EDPB Binding decision 1/2021 in the WhatsApp case: pt. 159: "*the DE SA considers that "consensus on the scope of the investigation should be reached at an earlier stage by the competent supervisory authorities than in the current stage of the draft decision. Therefore, before providing the draft decision of the ex officio procedure the DPC should have sought consensus regarding the scope of the procedure prior to initiating the procedure formally"*.			**Concepts 3 and 5** address this issue.
Effective procedure - documentation sharing among SAs	It is unclear what documents the LSA and the CSA must mandatorily share with each other.	The text should specify that all CSAs should be able to access all the documents that the LSA compiles in the course of a procedure (the 'case file'), and obligehe LSA to include every submission by the parties or piece of evidences in the 'case file'.					**Concept 7** (joint case file) addresses this issue.

General topic	Description of a specific problem under the general topic	Ideal solution	Article(s) involved (national, EU, or other)	Reference to specific noyb cases	References to EDPB documents / table	Comments	Proposed Solution
Effective procedure - SAs have a preference for cooperation via informal workflows in the IMI system	SAs tend to make more often use from informal workflows in the IMI system rather than formal workflows - e.g., requesting information via voluntary mutual assistance, without legal deadlines and legal consequences when the request is not adhered to.	The regulation should provide when SAs should make use of formal requests (formal mutual assistance, joint operations and formal consultation) so that legal deadlines and legal consequences cannot be ignored. In general, the IMI system should be more user-friendly: SAs have to send each other emails about important notifications (e.g., information requests) as such notifications may disappear in the enormous amount of notifications that SAs get from the IMI system regarding their cases (causing a huge chaos in tracking down the status of a particular case, for instance, because each new step within one case may be linked to a different case number).	Articles 60, 61 and 62 GDPR.				**Concepts 8 to 12** should addresses this issue.
Effective procedure - emergency procedure	The emergency procedure under Article 66 GDPR is rarely used 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.	The draft regulation should provide for an obligation to use the urgency procedure in cases referred to in Article 61(8) and 62(7) GDPR.	Article 61(8), 62(7) and 66 GDPR.			Problems with the urgency procedure (but also the 64(2) procedure in combination with 61(8) and 62(7)) is that SAs that trigger these mechanisms will often not have sufficient information to take a well-informed decision. E.g., when urgency is triggered because the LSA does not respond to a MA request for further information within the legal deadline, the CSA can probably not decide without such information.	**Concept 5** should be a suitable alternative.
Effective procedure - differences in confidentiality requirements among SAs	In theory, confidentiality requirements could hinder SAs to exchange relevant information in the IMI system with other SAs or the EDPB. The Lux SA, for instance, shall only be authorized to share information with these authorities on the condition that these authorities, bodies and persons are covered by an obligation of professional secrecy equivalent to that cited in their own national GDPR implementation act.	The regulation should ensure that SAs are not subject to confidentiality constraints to exchange information between SAs and between SAs and the EDPB, since all of them are already subject to confidentiality obligations under the GDPR, which are enough to support the exchange of information in full confidence. .		See Meta "forced consent" cases in Ireland where we understand that DPC refused to share information with other SAs. We see a wider trend to counter the transparency obligations under the GDPR with alleged "confidentiality" of any submission, legal argument or fact. Controllers seem to misuse valid arguments for protections to undermine fair procedures and party rights. This does nto make any sense, since once appeald before the court, all submissions and relevant documents of the administrative file will be shared with all parties under the rules applicable to judicial proceedings.			**Concepts 2** should take care of the matter. EU law on commercially sensitive matters are alreadyl unifying the protections.
Threshold for submitting a relevant and reasoned objection (RROs) is very high	As a CSA it might be very difficult to substantially reason an objection (especially when a CSA is not well informed about the case early on in the procedure by the LSA). Often CSAs then tend to submit comments, rather than RROs, or they merely submit an objection during 'informal consultation'. This clearly does not lead to the required peer pressure among SAs, as those SAs can ignore informal consultation or comments. Such decisions will, hence, also never end up at the EDPB dispute resolution mechanism.	The text should ensure that the LSA cannot simply ignore other views, comments and exchanges on the draft decisions, besides RROs.	Article 60 GDPR				**Concept 8** (defining Article 60 further) and **Concept 16** (definitions) could deal with this matter.
LSAs respond differently to RROs	Some LSAs submit a revised draft decision for a new round of consultation (as the GDPR requires), while other LSAs submit certain documents (such as composite memoranda) in which they respond to comments. Problematic for homogeneity in working practices.	The draft regulation should emphasize that a revised draft decision should be shared for a new round of consultation (including a deadline)	Article 60 GDPR				**Concept 8** addresses this issue.
Relevant information to share in the cooperation procedure	Article 60 does not define what should be shared with the other SAs (draft decision, complaints, submissions of the parties, attachments, evidence, inspection report, ..). The same is true about which documents must be shared with the parties in the context of the right to be heard	The regulationshould clarify what documents should be at minimum shared in the cooperation procedure of Article 60 GDPR. The text should also clarify that these documents should be shared with the parties for them to exercise their right and provide for limited exceptions under which they are cannot receive the submission.	Article 60 GDPR	See Irish case involving Meta where the Irish SA does not share all elements of the case with the other SAs and the EDPB (exclude some documents submitted by noyb, such as consumer studies or letters asking to extend the scope).		Inspiration can be drawn from the list of documents adopted in the Article 65(1)(a) guidelines and national policy documents on what constitutes 'relevant information'. Alternatively, list of documents needed for a 64(1) request could function as inspiration (a request cannot be submitted via the IMI system if not all relevant documents are uploaded).	**Concepts 7 to 10** address this issue.
VIII. EDPB level							
Procedural rights - right to be heard at the EDPB level	Rules of Procedure (article 11.2) mentions the right to be heard by the affected parties but the text should be further clarified as to: - what is subject to the right to be heard at national level - the EDPB should hear the parties again - all parties should be heard (complainant and controller) - should a hearing take place or just written submission - the deadline for the submission is not clear and should be reasonable	Both complainant and the controllers 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 at th enational level. The procedure is not composite and another round of right to be heard shoudl be organised, separate to the one organised at the national level.					**Concepts 7 to 10** address this issue, mainly by allowing a right to make a submission via the national SA as well as an option of the EDPB to hear the parties directly.

General topic	Description of a specific problem under the general topic	Ideal solution	Article(s) involved (national, EU, or other)	Reference to specific noyb cases	References to EDPB documents / table	Comments	Proposed Solution
Procedural rights - informing the parties about the consistency mechanism	Today, there is no obligation to formally notify the parties that a decision under the consistency mechanism has been submitted to the EDPB.	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 file access.		In the complaint on transfers against Facebook, but also in the three complaints against Meta (Instagram, WhatsApp and Facebook), we were not formally informed of the procedure triggered before the EDPB.			**Concept 8** includes this matter.
Added value of EDPB guidance documents (e.g. procedural guidelines) is unclear	Many statements within procedural guidelines are formulated in weak terminology often vaguely prescribing the required action of SAs. This is a result of the lack of unanimity among EDPB members: the text is always a compromise.	Many statements from the EDPB's procedural and internal guidance documents will have to be clarified before allowing their adoption within a procedural regulation. SAs can increase the authoritative character of guidelines by referring to it in their final binding decisions and publishing guidance on its website (creating legitimate expectations).	Article 70(1) GDPR.	See the Meta case where the DCP wrote that it was bound by the EDPB guidelines.			This is addressed by the Regulation overall.
EDPB deadline for decision-making is too short	A deadline of one month (potentially extended by a further month) is too little to take well-informed decisions. There is then no time to request additional information (in exceptional circumstances), translate those documents, organize hearings, request the EDPB approval for the inclusion of additional documents in the file, etc.	Deadlines of the EDPB should be extended when ecessary in exceptional cases. Examples can be found in other basic regulations from EU agencies with decision-making competences.	Article 65 and 66.				**Concepts 7, 8 and 11** should limit this problem.
EDPB binding directions too broad or disregarded	When implementing the EDPB decision, SAs 'must' follow the binding directions of the EDPB. These binding directions, however, are often broadly formulated, leaving a lot of leeway to the SAs to deal with it as they wish. E.g., a higher fine, does not per se lead to a fine that is truly high enough. The EDPB is, furthermore, not keeping an eye on the implementation of its decisions. All the SAs should do, is informing the Board about its final decision. If not followed, there is no tool in the GDPR that allows the EDPB to act (only possibilities are Commission infringement procedure, or CJEU).	EDPB should formulate its decisions in a way that leaves less discretion to the national SAs. EDPB should be able to step in when its decisions are not followed. Inspiration can be found within the SRB's regulation: if SRB's decision is not correctly implemented by the national authorities, the SRB can take over and directly address its decision towards the institution under resolution, see SRMR, Articles 18(9), 29(1), 28(1), 29(2).	Article 65.		See EDPB's first two binding decisions. More potential in its fourth decision where fine ranges where clarified.		**Concepts 8 and 11** should limit this problem.
EDPB lacks the competence to take well-informed decisions	The EDPB is a decision-making body but lacks any competence to collect information or evidence (striking compared to other EU Agencies with decision-making tasks). The EDPB is highly reliant upon the SAs, and can only hope for a complete file. It can indeed request further information from the SAs but only before the decision-making process is commenced and this information requested shall not be new information for the SAs. Highly problematic, as shown in the EDPB's first four binding decisions but also in the Meta cases based on noyb's complaints.	Text should allow the EDPB to request information from the SAs also during its decision-making process. Potentially even directly from the parties to the procedure if the SAs are unable to deliver the required information. Inspiration can be drawn from Article 35 of ESMA's regulation. For this, the Board would need more permanent members, not representatives from national SAs (also with an eye on potential conflicts of interests).	Article 65 and 66.				**Concepts 7, 8 and 11** should limit this problem.
IX. Communication and publication of final decision							
Procedural rights - the complainant is not always notified of the final decision or provided with a full copy thereof	Sometimes the complainants are not informed about the issuance of a final decision, including in the context of the OSS mechanism. Under Article 60(8) GDPR, the SA receiving the complaint should issue a decision on the complaint, even when the complaint is dismissed or rejected (see section IV above, "Obligation to issue a formal decision"). The SA should communicate the full decision to the complainant (including the decision of the LSA, as the case may be). It is up to the complainant to decide whether to appeal the final decision or not.	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.		e.g. 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.			**Concepts 9 and 11** address this issue.
Effective procedure - final decision: violation found but no action taken	Some SAs adopt a decision in which they confirm that a violation took place but still do not take any action.	The text should provide the obligation for SA to adopt a corrective measure when a violation is found, or justify why it did not adopt any (e.g. the violation has already stopped). If it fails to do so, there could be a presumption that the SA did not respect its obligation to handle the complaint with due care (cf. above, section III, "Holding SA accountable"). Such decision would be subject to judicial review.		Noyb recveived numerous reports regarding such "outcome letters" from the DPC, confirming that a violation of the GDPR took place, but inviting the complainant to go to court to enforce their rights.			While **Concepts 11 and 13** may help in this regard, it seems that current non-enforcement is more a matter of practice than law.

General topic	Description of a specific problem under the general topic	Ideal solution	Article(s) involved (national, EU, or other)	Reference to specific noyb cases	References to EDPB documents / table	Comments	Proposed Solution
Procedural right - Language of the final decision	Sometimes the language of the decision is different from the language of the complaint (especially in Member States with multiple official languages, 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 language of the complaint should define the language of the procedure, without prejudice to the translation of the document for the controllers, if necessary.		noyb 101 complaints lodged in Luxembourg: Complaints in German, decision in French. noyb complaints in Belgium against Instagram where the Belgian SA communicated in English and French, and shared the decision of the DPC with noyb in an email in English.			**Concept 2** leads to parties always communicating in the local language of the CSA/LSA they choose.
Publication of the final 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 or the Lux SA). - 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 text should provide for harmonised rules : - All SAs should publish any outcome of all cases (complaint or ex officio investigation, sanction or dismissal of the case) on their website. - Publication of the names of the contrrollers should not be seen as a corrective measure (not mentioned in Article 58 GDPR) - The names of legal persons should only be redacted where appropriate and in limited circumstances. - The names of complainants should always be redacted or pseudonymised, otherwise this would disincentivise complaints.					**Concpet 15** relates to this issue.
Redacted final decisions	The SAs have different approaches regarding the publication of their decisions. '- Some SAs redact the names of the controllers whereas some decide on a case-by case basis; '- Some identify controllers only as additional sanction (e. g. the CNIL / the Lux SA). 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.	The text should provide for harmonised rules regarding anonymisation, for example: - As a general rule, the names of legal persons should only be redacted where appropriate and in limited circumstances; - As a general rule, the names complainants should always be redacted or pseudonymised, otherwise this would disincentivise complaints.					**Concpet 15** relates to this issue.
X. Miscellaneous							
Collection of evidence	The collection of evidence (e.g. the duty to collect it, the rules on collecting files, witness statements and alike) should be regulated.	Law of SA collecting evidence applies					**Concept 2** leads to the local law applying.
Oral hearings	The use of oral hearings could often limit the need for hundreds of pages of submissions and ensure that procedures are focused on the core issues.	Law of SA hearing the parties/a party applies CSAs must have the possibility to take part if they want Data subjects must be heard in the language of their complaint No "secret hearings". If one party is heard, the other party must also be invited or at least be informed of the hearing taking place and be proactively provided with the minutes of the hearing					**Concept 2** leads to the local law applying.
Enforcement	Enforcement of final decisions against controllers: How precise does a decision have to be to be enforceable by the competent authorities? (How) can decisions by one SA be enforced in another member state?						**Concept 13** deals with this matter.
GDPR procedural priority rule	A certain set of processing operations can trigger different laws (concurrence of laws). For instance, when cookies are concerned, the installation of the trackers activates Article 5(3) privacy and its national transposition, including the SA's territorial and material competence. Whatever happens afterwards (further processing) triggers the GDPR instead. In some cases, this may be problematic. because ePrivacy rules are scattered and often inconsistent.	When the GDPR and other applicable law are concurrently applicable, we should propose some sort of "GDPR procedural priority rule". In other words, GDPR territorial and material competence should prevail and also cover the previous phase (see also next point).					There is no concept that directly deals with that. Under **Concept 2** the national law applies.