noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
AUSTRIA

28 June 2021

Dear [redacted],
Dear [redacted],
Dear [redacted],
Dear [redacted],

CC: [redacted]
CC: [redacted]

Subject: ***noyb*** **comments on the enforcement of the GDPR**

We would like to thank you again for meeting with us in February, when we had the opportunity to discuss several points related to GDPR enforcement, the one-stop-shop mechanism, and other issues encountered by *noyb.* Since the GDPR has just had its three year anniversary, we thought it would be useful to share with you some further comments on the enforcement of the GDPR.

We would like to focus on four issues, for which we will suggest some possible solutions:

- Enforcement of the GDPR, with a focus on one-stop-shop cases,
- Enforcement of decisions against foreign entities for violations of the GDPR,
- Funding for litigation in data protection cases, and
- Balancing of the right to data protection with the right to freedom of expression.

1. Enforcement of the GDPR and the one-stop-shop procedure: problems and possible solutions

In this section, we provide an overview of the issues we have encountered with the one-stop-shop procedures ("OSS") in the cases *noyb* has filed since May 2018.

1.1. Different issues identified

a. Lack of cooperation

At the core of many issues is a lack of actual "cooperation" by SAs. Despite the clear wording of the GDPR requiring the SAs to cooperate, SAs seems to largely engage in European ping-pong, shifting the work to the other SAs and minding their own business instead of engaging in proactive cooperation. The CSA usually just sends the case to the LSA and lets the LSA investigate the matter. Therefore, the CSA usually only acts as a "mailbox," merely transferring the correspondence to and from the LSA. In more and more cases the "mailbox" approach does not work; we have encountered caseswhere documents and submissions were lost or never even shared via the IMI system. Joint investigations or exchanges about a uniform approach are rare . Data subjects seem to be better off when directly filing with the LSA (giving up their right to use their national language and have an appeal in their jurisdiction) than using the OSS.

b. Application of different procedural laws

Complainants usually engage with the CSA in their Member State, their language and expect to have the local procedural law applied to their case.

However, LSAs equally apply their national language and national procedural law to the procedure (investigation, right of the complainant in the procedure, decision-making).

As a consequence, the same case may be handled by two SAs under conflicting procedural rules. As both parties have the right to appeal a decision, including on procedural grounds, this may even lead to different standards during the judicial review of the same procedure. The complainant whose complaint has been rejected can appeal the decision of the CSA before the national court. This court will usually apply its local administrative procedural law when conduction such a review, which may have not been followed by the LSA during stages of the procedure.

For example: The French CNIL takes the view that a complainant is not a party to the procedure and the Irish DPC takes the view that it must not disclose the submissions by the controller to the complainant. Austrian or German procedural laws require full engagement of all parties and disclosures to all parties. A negative decision of the SAs would be issued by the CSA and appealed before the Austrian or German courts who would have to apply the Austrian or German procedural law and likely thereby have to invalidate the decision, as the complainant was not granted a fair procedure.

c. Role of the complainant as a party to the procedure

Some national procedures make the complainant a participating party in the procedure (e.g. Austria, Belgium, Germany Ireland or Spain), whereas in other jurisdictions, the complainant is not even allowed to intervene in the procedure (e.g. France and Sweden).

This may lead to situations where the complainant will not be allowed to make a submission in the course of the procedure even though the procedural law of the LSA (e.g. the Belgian DPA) actually *does* provide for such a possibility. Consequently, the complainant might be deprived of the right to be heard under Articles 77 and 78 GDPR and Article 41 of the Charter.

In cross-border cases, this may lead to a fundamentally different treatment of complainants, depending on the SA that the complaint was filed with. A German complainant may get full party rights against a French controller, while a French complainant would not be seen as a party in a complaints procedure against the same controller.

For example: The French CNIL takes the view that a complainant is only petitioning the CNIL but has neither a right to a decision, nor a right to engage in any procedure the CNIL may initiate on foot of a complaint. In a case we filed with the CNIL, we got an informal email with a link to the CNIL's website, informing us that Google was fined € 50 million on foot of a complaint. There was no engagement after the filing of the complaint until the decision was issued.

d. Duty to decide on complaints

We observe an increasing number of SAs taking the view that they have no obligation to adopt a binding decision after a complaint. This view was publicly expressed by the Irish DPC,[1] was subject to a lawsuit in Luxembourg, and is currently under discussion in Belgium.

While there are reasons to reject cases *for technical reasons* (for example when complaints do not fulfil the minimal requirements or when the SA is not competent), SAs may not simply "ignore" complaints or "pick and choose" which complaints to investigate. It would be absurd if the EU would on the one hand grant a fundamental right to data protection and privacy in the CFR, while the relevant authorities take the view that such rights cannot be enforced in practice.

We think that this practice is, among other things, contrary to the *Schrems I* and *Schrems II* CJEU judgements (confirming that SAs have the duty to act), Article 57(4) GDPR (outlining limited cases where SAs can refuse to act), and Article 8, 41 and 47 CFR. To make it simple: The current situation is like having a right to vote, but in some Member States there are simply no voting booths that would accept and tread cased votes.

Since SAs have different opinions on the matter (sometimes explained by a lack of resources, sometimes as a matter of convenience, or argue to be subject to different national laws regarding their obligation to act) such loopholes create an avenue for forum shopping by controllers. Controllers can decide to establish in countries where the SA does not act on complaints.

For example: The Austrian DSB or Spanish AEPD publishes numbers about the handling of all complaints they received. Some cases are initially rejected as they do not fulfil formal requirements of a compliant, others are referred to other LSAs, some are resolved during the procedure (like when a controller provides the relevant data under Article 15 GDPR) and the rest recieves either a positive or negative decision. At the same time the Irish DPC or French CNIL take the view that they do not have any duty to decide individual complaints and may pick and choose the cases they investigate. The Irish DPC revived 10.150 complaints in 2020 but has not made a formal decision on any GDPR complaint in 2020.

e. Informal "closing" of cases

A closely related issue is thatsome SAs also take the view that they must handle a complaint, but that "handling"canmean just closing cases without any further investigation and without giving any reason.These SAs usually also argue that complainants have no right to appeal a decision to close a case, as SAs did not have a duty to act anyway. Following their arguments, the judicial review provided for in Article 78 only exists when the SA (1) has not dealt with the complaint at all (so not even "closed" the case) or (b) has not informed the complainant of the progress (which is usually the mere information that the complaint is still "open", see below).

This is contrary to the clear intent of the legislator in light of Article 8, 41 and 47 CFR and Article 78 GDPR. In addition, the case of a cross border complaint, Article 60(8) GDPR explicitly requires a "*decision*" when SAs "*dismiss or reject*" a complaint. It would make no sense and would be discriminatory to deny this right to the complainant when the case does not involve a cross border situation.

For example: The Irish DPC usually sends data subjects emails where they simply inform the complainant that they do not plan to further engage with them. When asked about the legal nature of such emails, the DPC denies that this would constitute a decision.

[1] See e.g. https://noyb.eu/en/irish-dpc-handles-9993-gdpr-complaints-without-decision

f. Update on the status of a complaint

Article 77(2) GDPR obliges the SAs to inform the complainant on the progress and the outcome of the complaint. Article 78 GDPR gives the complainant a right to an effective judicial remedy in case they are not informed about the progress or outcome of the complaint or if the complaint is not handled by the competent SA. In most cases, we do not receive regular updates from the SAs at all, even several months and sometimes years after filing the complaint, and despite several reminders.

If we receive updates, the updates are limited to a mere notification that the investigation is ongoing and that the SA needs more time. More substantive updates are rare and limited to certain SAs. It is more likely to get a normal procedural document, whenever that is issued, than an actual update within the meaning of Article 77(2) GDPR.

For example: The Austrian DSB usually adds a text block to any document sent to the complainant, saying that this document is the required "*information under Article 77(2) GDPR*". There seems to be no routine to update complainants within 3 months.

In some cases, it seems that it is not even clear to the SAs which SA is in charge of informing the complainant about the status of the complaint. We usually encounter the "information" that there is "no new information" by the LSA, whenin fact the LSA is conducting a procedure.

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 order the SA to inform the complainant as per Article 77(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 impact the procedure or on the inaction of the SAs.

In summary 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 substantive information, and courts require such substantive information.

g. Language of the procedure

We also encountered several cases where the use of different languages in cross-border cases was causing multiple procedural issues.

In practice, the LSA conducts the investigation and the outcome is then shared with the CSA in the original language and in English. In most cases, the documents of the LSA are translated into the language used by the complainant. These translations are often mere "machine translations" which are hard for an average citizens to understand, especially when the automated tools translate legal jargon. Even with a multi-lingual team of lawyer, we were regularly unable to make any sense of such translations by the CSA and instead requested the original document from the LSA. On the other hand, manual translation often takes months to be finalised.

For example: The German BfDI took up to two months to manually translate English documents by the Irish DPC into German. The Austrian DSB delivered machine translations of a submission by a Slovak controller instantly, but the quality was so poor that our lawyers were merely guessing what the controller had argued, fundamentally undermining the party's right to be heard.

In addition, some SAs refuse to translate documents into local languages. This amounts to a violation of the principle of proximity, which enables any individual to file a complaint with their local SA in one of the official languages of the country, in order to enforce their fundamental rights. Such procedures also do not respect the right to be heard and the right to good administration, since the complainant cannot submit observations in their own language.

For example: The Irish DPC and the Belgian SA ended up handling a French complaint that was filed in Belgium in English. The Belgian SA refused to translate the inquiry report of the Irish SA into French. Even more, the language used between the Belgian SA and *noyb* in the course of the procedure was English, despite the strict laws regarding the use of languages in Belgium.[2] In any appeals situation, the Belgian courts would likely be unable to work with the documents of the procedure. The Irish DPC in turn used our request to have these documents delivered in the legally required language as an argument that we would have obstructed the procedure before the Irish courts.

h. Access to documents

Article 41 of the Charter provides for a right to good administration, which in turn consists of a right to have access to documents. However, we have observed that the SAs do not consistently answer our requests to access documents relevant to the procedures in which we are involved.

Some SAs share only selected documents and files with other SAs. We observe that some SAs even leave their European colleagues in the dark and do not exchange documents in time.

In some cases, the exchange of documents with the SA is even refused by LSAs. This leads to situations where parties cannot access documents via their local SA because it has simply never received the documents from its counterparts.

When documents are properly shared by the LSA with the CSA, the national law applying between the complainant and the CSA should regulate the access to documents. Nevertheless, some LSAs try to have their procedural rules apply abroad, *e.g.* by simply not providing the documents, requesting that documents are not shared with the parties or by requesting that documents be deemed "confidential". The limited sharing of documents makes it partly impossible for CSAs to comply with the applicable procedural law between the CSA and the complainant.

For example: The Irish DPC took the view that it must not share documents with the Austrian DSB, the German BfDI and the complainant. Requests by the Austrian DSB and German BfDI were ignored and we could consequently not exercise our right to access documents within Austria and Germany, as the DSB and BfDI simply did not get these documents from the Irish DPC. Our request to use Article 61(1) GDPR to formally request these documents from the Irish DPC were rejected, as the Irish DPC claimed that we have no right to request such actions by the CSA. This matter is currently under appeal in Austria.

Another example: As a controller (Facebook) deemed its legal arguments (e.g. the legal basis Facebook relies on under Article 6(1) GDPR) to be "confidential", the DPC required us to not disclose the content of these documents, despite the fact that there is no legal basis for such an order under Irish law. In addition, we received these documents via the Austrian DSB under Austrian procedural law and the Austrian DSB informed us that there is no legal basis in Austria to limit the use of documents that we get via public authorities.

[2] See also Decision interlocutoire 26/2021 regarding a complaint against IAB, where the Belgian SA chose English as the language of the procedure because the IAB, with main establishment in Belgium, preferred to use English as the language of the procedure. The Belgian SA disregarded the position of the complainant, as the SA did with *noyb*, considering that our NGO proved that it could communicate in several languages, whereas it is obvious that the same conclusions could easily be reached regarding Facebook, against whom the complaint was filed.

i. Timelines

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.

This lack of timeline leads to inaction from SAs when it comes to:

- the transfer of complaints to the LSA (in some cases, CSAs only forward the complaint several months after the complaint was lodged);
- starting 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.

Numerous individuals come to *noyb* to complain about the lack of action of the SAs and do not know to who to turn to enforce their rights. The OSS has quickly become a "black hole" where complaints disappear for years. This situation creates a lot of prejudice against the promise of a new era of enforcement and digital rights made by the Commission with regard to the GDPR.

j. Inaction of an SA and "urgency"

Considering that some GDPR violations may persist for years before a final decision is adopted by the LSA, the EDPB, or perhaps even the CJEU, the SAs should be encouraged to implement the urgency procedure foreseen in Article 66 GDPR.

To our knowledge, this procedure has only recently been triggered in two cases,[3] while the effectiveness of this procedure has been recognised by the Advocate General Bobek and the Court in the case between Facebook and the Belgian SA.[4]

In our experience, SAs promote a very narrow interpretation of urgency, where Article 66 GDPR should only apply in "life or death" situations. However, most GDPR cases concern the ongoing violation of the fundamental rights of a large number of data subjects and are therefore "urgent". Cases can also become urgent when there is a continuous violation and no action by the LSA.

The legislator clearly had another idea, as urgency under Article 66 GDPR is automatically triggered in cases where an SA does not answer a request from another SA under Articles 61 and 62 GDPR.[5] This is at odds with the view of many SAs for a limited understanding of urgency.

Further there seems to be a lack of remedies when a foreign LSA is not acting, as any judicial remedy against the CSA usually leads to the CSA to pointat the LSA and a procedure against the LSA would require the complainant to engage in a procedure in another Member State, which is in practice almost never happens. The LSA therefore has little to fear when ignoring complaints

[3] See decision of the Hamburg Commissioner for Data Protection and Freedom of Information, 'Urgency procedure opened against Facebook in connection with the new WhatsApp terms of use', 13 April 2021. See also the decision of the Italian SA regarding TikTok: https://edpb.europa.eu/news/national-news/2021/italian-dpa-imposes-limitation-processing-tiktok-after-death-girl-palermo_en.
[4] Case C-645/19, Opinion of the Advocate General delivered on 13 January 2021(1), cf. paras. 118, 135.
[5] Which is the case in the decision of the Hamburg Commissioner.

that were filed abroad – unless the CSA would have a duty to use the relevant tools to force the LSA to take action

For example: In cases on so-called "forced consent," the Irish DPC has not issued a decision for more than three years. The German and Austrian SAs take the view that they cannot use the urgency procedure to require the Irish DPC to take certain steps, as a continuous violation would never be urgent. The complainant therefore has to file a judicial review against the Irish DPC before the Irish High Court – costing up to € 200.000 to "kick start" the procedure in Ireland, even when filing the complaint at the local SA in Germany or Austria.

1.2. Possible solutions

Apart from being able to monitor the correct implementation of the GDPR by the Member States, we hereunder list some of the options that the Commission could contemplate to address the issues identified above. We urge the Commission to take a proactive role in overcoming the known issues of the GDPR, as some SAs seem to have an inherent interest in not overcoming these issues and not limiting their own discretion.

a. Request EDPB Opinions (Article 64(2) GDPR), guidelines, recommendations and best practices (Article 70(1)(e), (l) GDPR)

It is obvious that the Commission has a unique role as an external "**pace maker**" when some SAs may have an interest in keeping these issues unresolved. The GDPR gives the Commission various options to kick start major improvements when the EDPB may be paralyzed:

Article 64(2) GDPR allows the Commission to *"(…) request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62".*

The scope of Article 64(2) GDPR is not limited to specific issues or cases ("*in particular*"). Therefore, the Commission can request the EDPB to adopt an opinion, *i.e.* on matters related to complaints-handling procedures, the definition of key concepts, deadlines, cooperation mechanisms, translation and other such issues. Under Article 64(2) GDPR, such an opinion must be issued within 14 weeks.

Article 70(1)(e) and (l) GDPR allow the Commission to request the EDPB to *"examine (…) any question covering the application of [the GDPR] and issue guidelines, recommendations and best practices"* in order to encourage the consistent application of the GDPR.

The Commission could use this option to ask the EDPB to make the handling of cross-border cases more efficient and harmonised across the EU.

According to the Commission's evaluation report on the two years of the GDPR ('2020 evaluation report'), the EDPB has already started *"a reflection on how to address [these] concerns".* The Board will *"clarify the procedural steps involved in the cooperation between the lead data protection authority and the concerned data protection authorities, analyse national administrative procedural*

laws, work towards a common interpretation of key concepts, and strengthen communication and cooperation (including joint operations)".[6]

- The Commission could therefore request a regular status update from the EDPB on the progress of work conducted by the EDPB and its planned timeline. As the Commission pointed out in its 2020 evaluation report, the EDPB is an EU body and must apply EU administrative law and ensure transparency in the decision making process.
- In light of the Commission's statement in the 2020 evaluation report that it will *"support the reflection within the Board on the procedures applied by the national data protection authorities in order to improve the cooperation on the cross-border cases"*[7], we would like to encourage the Commission to provide to the EDPB as much assistance as possible to achieve the set goal.
- Apart from the mechanisms mentioned above, the Commission may also consider using other "soft methods" to encourage stronger and more effective enforcement of the GDPR, e.g. via mutual assistance agreements and letters of understanding between willing SAs.

More specifically, the Commission could ask the EDPB to clarify the issues raised here above. In this context, the EDPB could be asked to:

- publish an overview of all procedural laws and practices applicable to the procedures before each SA to ensure better access to this information by the SAs and by the public,
- adopt an opinion on how to deal with cases where different national procedural laws apply (e.g. clarifying that the LSA and CSA apply their national procedural law, which defines the language to be used, the access to documents and role of the complainant in the procedure),
- clarify that the SAs must ensure that LSA and CSAs get all relevant support and information to enable them to comply with national procedural law,
- clarify whether the SAs have to adopt a decision pursuant to a complaint and to which extent these decisions are subject to effective judicial redress by the complainant,
- set a standard period within which documents should be shared to all CSAs via the IMI system,
- adopt an opinion defining the circumstances when the SAs should trigger the procedure under Article 66 GDPR.

Given the political reality, we especially want to highlight that a first step could be to frame these rules as "**recommendations**" or "**best practice**", which would have political and practical meaning and give legal certainty to SAs, while allowing certain flexibility when there are overriding conflict of law issues or practical limitations.

For example: A recommendation could say that a cross-border case usually follows certain steps and certain timelines (e.g. initial review of the admissibility of the complaint by the CSA, forwarding within two weeks, a response by the controller within one month, communication of the response to the CSA and complainant within a week, joint determination of open issues and necessary investigations or submissions, two months from the closing of the investigation until a draft decision is issued via the Article 60 procedure). While SAs may depart from this recommendation in a given case, it would allow SAs to expect certain steps to be taken in a certain time, while also giving them legal certainty in the case of judicial reviews.

b. Infringement procedures

The Commission could consider launching an infringement procedure against a Member State under Article 258 TFEU to ensure that the Member State complies with the EU law.

[6] Commission Staff Working Document, 24.6.2020 SWD(2020) 115 final, Brussels, p. 10.
[7] Communication from the Commission to the European Parliament and the Council, 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation{SWD(2020) 115 final}', 24.6.2020 COM(2020) 264 final, Brussels.

For example, the Commission might start an infringement procedure in countries where:

- The **right to be heard** and the **principle of proximity** are violated by an SA that refuses to communicate with complainants in their language.
- **Sufficient resources** are not provided to the SAs in order to facilitate their exercise of powers under the GDPR or if the GDPR is not implemented or enforced in any other way.
- An **SA systematically does not act after a complaint** or decides to close a case.
- It is **not possible to appeal the decision of an SA** closing a case or rejecting a complaint.

We want to highlight the resolution P9 TA(2021)0256 by the European Parliament from 20.5.2021, requesting the Commission to take action against the Republic of Ireland and the open acknowledgement by the Irish DPC that is takes the view that "handling" of a complaint may mean to not take action.[8] This approach is also apparent from the DPC's Annual Report, which lists 10.150 complaints filed with the DPC directly in 2020 and no decisions that were based on these complaints.

c. Comparing the enforcement activities of the SAs with their annual report

The annual reports of SAs are essential to provide the Commission and the public with the information necessary to prepare the evaluation report on the GDPR, to measure the performance of each SA, and to understand how the GDPR is enforced in the different Member States.

According to Article 59 GDPR, the annual reports should list the of types of infringement notified and types of corrective measures taken in accordance with Article 58(2). In our experience, apart from often being not easily accessible, the SAs' reports do not provide information in a harmonised way about the measures they adopted.

For example: The very definition of a complaint differs from one Member State to another, and is therefore counted differently in each annual report. Some SAs reported complaints as "concluded" even when they were never investigated or decided upon. Others transparently split reporting numbers by initially rejected complaints (e.g. for formal reasons), complaints that became moot during the procedure (e.g. when access was granted during the complaints procedure) and upheld/rejected complaints. Human resources are sometimes expressed as the number of people working within the SA, while in other cases they are expressed as the number of full-time equivalents. The job descriptions and training of personnel are rarely reported, making it hard to compare the level of expertise of different SAs. Budgets are often not reported on in the annual reports.

As a solution, the Commission could request the EDPB, under Article 70(1)(e), to draw a standard list of statistical elements and their definitions to ensure that all SAs report on the same issues in their annual reports. This will make such reports comparable and useful.

2. International enforcement

One issue that *noyb* has identified is the problem of enforcement of the GDPR by the SAs against foreign entities (*i.e.* entities that do not have an establishment in the EU).

The extraterritorial scope of the GDPR, as is provided under Article 3(2) GDPR, allows for the application of provisions to non-EU operators who process the personal data of European individuals. Article 27 GDPR stipulates: "*Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.*" Despite this, some SAs are reluctant to

[8] https://noyb.eu/en/irish-dpc-handles-9993-gdpr-complaints-without-decision, we are happy to provide the Commission with a full transcript of the hearing. The transcript can also be demanded from the Irish Parliament.

investigate cases and/or adopt enforcement measures where a controller does not have an establishment in the EU,their own Member State, or province within the Member State.[9]

In this respect, they are rarely decisions and measures adopted against companies for failing to appoint a representative in the EU (Article 27 GDPR).[10] As the Commission is well aware, the appointment of a representative by non-EU organisations subject to the GDPR is necessary to aid the extraterritorial application of the GDPR and its enforcement in practice. However, the ongoing legal debate about the possibility for SAs to impose corrective measures (and fines) on the representative may lead to some doubts about the added value of the obligation to appoint a representative. To the contrary, it seems that controllers may avoid appointing a representative to escape the GDPR fully.

2.1. Enforcement within the EU against a controller or processor established in another Member State

The issue of enforcement already exists within the EU. For example, when a SA imposes a fine against a controller that is not established in its territory.[11] In our practical experience there is vast uncertainty about how an SA may impose a fine when it has jurisdiction under the GDPR, but the controller resides outside of its Member State.

2.2. Enforcement outside of the EU

Enforcement Article 29 Working Party stated that cross-border cases in data protection law are *"a general question of international law"*.[12] To our knowledge, there are currently no binding international agreements between the EU and other countries that stipulate the (mutual) recognition of administrative decisions of SAs or courts in data protection and privacy cases.

Article 50 GDPR creates a framework to develop mechanisms to achieve actual enforcement of the GDPR fines and administrative decisions on a global level. However, it seems that this is still a missing element which needs to be seriously considered and acted upon by the EU Commission.

2.3. Possible solutions

- The Commission could encourage SAs to use existing legal enforcement instruments, such as freezing an infringing company's assets, blocking of websites, setting national procedures to recover fines, putting in place international mutual assistance instruments, etc.
- The EU adopted a Framework Decision on the Application of the Principle of Mutual Recognition to Financial Penalties[13] to ensure the enforcement of penalties issued by the authority of a Member State within the EU. To our knowledge, this mechanism has never been applied to the enforcement of the GDPR. The Commission could also take action to make sure that the available legal instruments are effectively used.

---

[9] See the case of the CNDP in Luxemburg, on our website. See also annual report of the SA of Saxe for 2019, p. 109, 5.2. Similar issues were encountered with the Hamburg DPA, when a complainant filed a case against a US company that processed data from all EU Member States, but the Hamburg DPA was limiting any decision to Hamburg residents.

[10] The only case we found is the Locatefamily.com case of the Dutch SA where the AP imposed a fine for lack of representative.

[11] See cases where one-stop-shop does not apply: Articles 55(2), 56(2)-(6) and 66. In such cases, the SA may have to impose a fine on a controller with no establishment on their territory.

[12] Article 29 Working Party, 5035/01/EN/Final WP 56, p. 2.

[13] Council Framework Decision 2005/214/JHA of 24 February 2005 on the Application of the Principle of Mutual Recognition to Financial Penalties.

- Especially in relation to foreign entities with no direct assets in the Union, we would like to highlight the option to enforce penalties against third parties (such as banks where a controller holds accounts), which is regularly used in other areas of the law ("garnishment").
- The absence of mechanisms to enforce SA and national court decisions in non-EU countries should be addressed by the EU Commission using its powers under Article 50 GDPR.
- The Commission should also take suitable action to encourage enforcement of the obligation to appoint a representative in line with Article 27 GDPR.
- In the same vein, the Commission should clarify the powers of SAs vis-à-vis representatives appointed according to Article 27 GDPR.

3. The need for a sustainable and accessible funding for litigation

Both the Commission[14] and the European Parliament[15] recognise that further progress is needed in the field of the GDPR enforcement.

The GDPR offers a range of enforcement mechanisms, from the option to file a complaint with an SA, *ex officio* investigations, legal proceedings in courts by individuals, to collective redress in some jurisdictions. Enforcement actions handled by SAs have had very limited effect in some key Member States, such as *e.g.* Ireland and Luxembourg, which act as lead authorities for the enforcement of the GDPR vis-à-vis big tech companies.

Insufficient funding for SAs might be one reason why the GDPR is not being successfully enforced. However, the problem is even more systemic; we also observe some reluctance from SAs to go against bigger controllers to avoid the work and cost that would be generated.

Therefore, legal proceedings filed by NGOs and consumer organisations are of utmost importance. This is recognised by Article 80(2) GDPR and the new directive on representative actions adopted in 2020. It is therefore crucial that civil society organisations (CSOs) have the financial capacity to engage in litigation.

Already in its 2018 Report, the European Union Agency for Fundamental Rights (FRA) highlighted the problem of access to funding for litigation in fundamental rights cases by CSOs.[16] The funding opportunities currently available for litigation in digital rights violations cases (e.g. by the Digital Freedom Fund, *DFF*) often have vague or unrealistic selection criteria for the litigation of GDPR violations. Funders are often reluctant to fund individual cases and do not cover adverse cost orders, which is a risk one needs to count with when litigating in certain jurisdictions.

The Commission itself seems to already be aware of the importance and the need of an independent and accessible source of funding for litigation by CSOs in fundamental rights cases. In the 2020 feasibility study for DG Justice and Consumers, the authors highlighted that the Commission's financial support for litigation in fundamental rights cases (incl. data protection cases) would add substantial value because *"there is a clear need for funding for such litigation, there are opportunities to advance fundamental rights jurisprudence, and such funding would be*

[14] EU Commission, 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation', 24.6.2020 COM(2020) 264 final, Brussels.
[15] Motion for a Resolution to wind up the debate on the statement by the Commission pursuant to Rule 132(2) of the Rules of Procedure on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application(2020/2717(RSP)).
[16] EU Agency for Fundamental Rights, 'Challenges facing civil society organisations working on human rights in the EU', p. 32.

within the scope of Commission grants architecture"[17]. We affirm this view and we propose that the Commission considers the following solutions.

Possible solutions

- The Commission could launch a new grants programme[18] to help CSOs do litigation where EU law is violated (incl. the Charter of Fundamental Rights and the GDPR), and to help CSOs obtain training and capacity-building to explore other remedies and redress mechanisms to enforce fundamental rights at national and European level.
- The Commission should closely follow how Member States will implement Article 20 of the representative actions directive 2020/1828, and in particular to how they provide adequate public funding to the qualified entities.

4. Civil Litigation

In addition to the matters of administrative complaints, we would like to draw your attention to the matter of civil litigation. In many cases, SAs refer to the civil courts as the alleged "main" path for a data subjects to enforce their rights. Nevertheless, we see vast pushback from civil courts to engage in data protection matters as they often see fundamental rights as being more of a political than a civil law matter.

4.1. Blockade of Civil Litigation

The legal literature (mainly written by industry lawyers) has developed various theories that are intended to block access to the courts, be it that data subjects could only enforce rights under Chapter 3 of the GDPR (but e.g. not a violation of Article 5 and 6) or that they are not entitled to non-material damages, contrary to the legislator's intent. We see these trends mainly in Germany and in publications by international law firms, but they are happily taken on board by courts, as it allows judges to dismiss complex GDPR cases, without dealing with the material questions of the GDPR. Industry lawyers circulate these opinions across jurisdictions.

Another major obstacle for data subjects in civil courts are costs. It is almost impossible to find lawyers that would represent data subjects, as almost all GDPR experts work for the industry and are therefore conflicted. If a law firm agrees to take a case, it comes at substantial costs for the plaintiff, as these cases are usually complex and controllers use every option to delay and complicate procedures. Judges request expert witnesses or reject cases on procedural grounds. In practice, this seems to be mainly a matter of disbelieve in the GDPR and a lack of training on the GDPR by parts of the judiciary, which makes judges avoid such cases.

For example: Litigation by Mr Schrems against Facebook in Austria went before the Austrian Supreme Court twice, as the initial local judge (unlawfully) rejected the case twice on procedural grounds. Only after five years, the initial judge finally accepted her jurisdiction for the case. Lawyers mentioned that clarifying the jurisdiction was too expensive for normal clients, so they waited for our case to be decided before even considering to litigate their own cases. This leadto major chilling effects in all Austrian courts.

[17] Lipson, Morris; Noorlander, Peter, 'Feasibility Study for financial support for litigating cases relating to violations of democracy, rule of law and fundamental rights', 29 June 2020.

[18] In fact, under the previous Justice Programme (JUST-2014-2020) the Commission had already made available a grant 'Capacity building for litigating cases relating to democracy, rule of law and fundamental rights violations' (JUST-PPPA-LITI-AG-2018). We strongly advocate in favour of a relaunch of a similar grant on favourable conditions with simple grant-making procedures, low application thresholds and, preferably, an absence of co-funding requirements.

In most cases, the costs paid by the losing party do not compensate the costs of the plaintiff. We currently estimate that any civil case costs *noyb* about € 20.000 to € 50.000, even when winging the case in the end, as the compensation is usually substantially lower than the actual costs of complex and lengthy GPDR litigation.

4.2. Non-Material Damages

When a data subject needs to litigate for years only to get a declaration that a controller should e.g. not have shared data, or should have better informed the data subject, it is nothing but a waste of time and money to enforce rights under Article 79 GDPR. In many cases, controllers make a case "moot" by providing the information years later in submissions or by deleting data during the procedureso that, for example, access can *de facto* not be granted or enforced anymore.

This is where non-material damages play a major role in compensating for wrongdoing that cannot otherwisebe compensated.

The legal industry is also attacking the intent of the GDPR in this area. It seems to us that a pre-GDPR doctrine in Germany is making its rounds in other Member States too; based on national case law on the right to personhood under the German constitution ("Allgemeines Persönlichkeitsrecht"), German legal literature has traditionally rejected non-material damages under Directive 95/46. On this national tradition, the legal industry now promots the doctrine that data subjects should only get emotional damages in severe cases and/or when they have suffered emotional distress that is equivalent to an infringement of the mental integrity of the data subject – so a violation of Article 3 CFR – while a "mere" violation of the right to data protection under Article 8 CFR would not lead to emotional damages. In practice, this means that data subjects would usually not be able to claim damages for GDPR violations, renderingany form of civil law enforcement beyond a mere declaration impossible in most cases.

We were informed that the Austrian Supreme Court (OGH) has referred the matter the CJEU, as it seems to depart from previous Austrian case law under Directive 95/46,granting emotional damages without any requirement of "substantial" damages under the impression of the German doctrine. The case is registered under C-300/21.

Background of the case: The Austrian Postal Service has illegally generated data about the possible political believes of mail recipients, to sell this data to political parties for mail marketing purposes. The data got deleted and the Postal Service de facto accepted that it acted unlawfully. As the data got deleted the Postal Service claims that is cannot give access to the data anymore and cannot inform data subjects about the recipients of these political profiles. A fine of € 18 million by the Austrian DSB was overturned by the Courts on procedural grounds. The plaintiff in this case asked for non-material damages as these profiles were generated about him and likely shared, but the Postal Service relied on a doctrine of "major distress" to argue that the plaintiff was not entitles to non-material damages – leaving the plaintiff with nothing but a declaration and costs.

We kindly ask the Commission to exchange with us on this case and to make submissions with the CJEU to ensure that the legislators' intent when implementing non-material damages in Article 82 GDPR is upheld by the CJEU.

5. Other matters: the right to data protection and the freedom of expression and information in the EU

As was mentioned in the Commission's 2020 evaluation report, the balancing of the right to data protection with freedom of expression and information, and of these rights required by Article 85(1) GDPR, may constitute a challenge to the national legislation.

Member States across the EU have different approaches to these two rights, with some giving precedence to the freedom of expression, and others to the protection of personal data.

In its 2020 evaluation report, the Commission stated that it:

> *"(…) will continue its assessment of national legislation. The reconciliation must be provided for by law, respect the essence of those fundamental rights, and be proportional and necessary. Data protection rules (as well as their interpretation and application) should not affect the exercise of freedom of expression and information, for instance by creating a chilling effect or putting pressure on journalists to disclose their sources. The balancing of these two rights by national laws should be framed by the case law of the Court of Justice and of the European Court of Human Rights".*[19]

We would like to bring to the Commission's attention two examples of Member States having translated this balancing in their national law, in a way that is not compliant with the GDPR:

4.1. The example of Austria

Article 9 *Datenschutzgesetz* ("DSG", the Austrian Data Protection Act) implements Article 85 GDPR.

Specifically, Article 9(1) DSG provides that Chapters II-VII and Chapter IX GDPR are wholly inapplicable with regard to the processing of personal data for "journalistic" purposes by media, according to the *Mediengesetz* (the Austrian Media Act).

Article 9(1) DSG law does not foresee any proportionality assessment, despite the explicit wording of Article 85(2) GDPR ("*Member States shall provide for exemptions or derogations (…) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information*").

[19] *Ibidem*.

4.2. The example of Sweden

Sweden typically places freedom of the press and freedom of expression above the right to protection of personal data.

Quoting from the Swedish SA's (IMY) website:[20]

> *"Where freedom of the press and freedom of expression are concerned*
>
> *The Freedom of the Press Act and the Fundamental Law on Freedom of Expression are constitutional laws that take precedence over other legislation. The General Data Protection Regulation permits EU Member States to make exceptions from the rules governing processing of personal data if it is necessary in order to maintain the right to freedom of expression. This means among other things that some media that are protected under the provisions of a constitutional law are exempt from review under the General Data Protection Regulation. This applies, for example, to personal data published on the daily newspapers' websites and DVD discs with a responsible publisher. In the case of violations in the area of freedom of the press you must contact the Press Ombudsman (PO) or the Office of the Chancellor of Justice (JK).*
>
> *Certificate of publication for a website*
>
> *If you have a website, you can apply for a certificate of publication. The certificate of publication gives the website protection under constitutional law, which means that publication of personal data is exempted from the General Data Protection Regulation. You apply for a certificate of publication from the Swedish Press and Broadcasting Authority."*

What needs to be underlined is that the requirements to be granted a 'certificate of publication' are so broad that any interested party can obtain one, and so no true proportionality assessment takes place, despite the clear requirement of Article 85(2) GDPR.

As the Swedish Authority for Press, Radio, and TV explains on their website:[21]

> *"Criteria for obtaining a publishing certificate*
>
> *In order to obtain a publishing certificate, the website or database must meet the following criteria:*
>
> - *It is available to the public.*
> - *It is provided on special request, i.e. the visitor actively seeks it out.*
> - *It is well delimited and appears as a cohesive product, for example through uniform design.*
> - *It cannot be changed by anyone other than the editors.*
> - *It has a name that contains a domain name.*
>
> *In addition, the website or database must also meet the following:*
>
> - *It should be connected to Sweden, for example because the editorial office is located here.*
> - *It must have a responsible publisher.*
> - *It must have a name that cannot be confused with any other database registered with us."*

[20] https://www.imy.se/other-lang/in-english/about-us/what-the-swedish-data-protection-authority-does-not-do/

[21] https://www.mprt.se/regelverk/utgivningsbevis/ (autotranslated using Google Translate)

The consequence of these low requirements is that a number of commercial services offer expansive databases on virtually all residents of Sweden, which include information such as:

- Full name
- Date of birth
- Residential address
- Other residents of the address
- Phone number
- Make and model of vehicles registered in their name, if any
- Pets registered in their name, if any
- Married or not
- Taxable income
- Companies registered in their name, if any

Examples of services are:

- https://www.hitta.se/
- https://www.eniro.se/
- https://www.merinfo.se/
- https://www.ratsit.se/
- https://lexbase.se/
- https://mrkoll.se/

Under Swedish law, the certificate of publication gives these services an absolute right to publish information without regard to the rights of the affected data subjects and under the guise of freedom of expression:[22]

> *"Can I demand that information about me on Mrkoll, Eniro, Hitta.se, Lexbase, Ratsit and Merinfo be deleted?*
>
> *No. Sites like MrKoll, Eniro, Hitta, Lexbase, Ratsit and Merinfo, among others, have something called publishing certificates. This means that the sites are not affected by the provisions of the Data Protection Ordinance, which means that the Privacy Protection Authority cannot help you.*
>
> *What you can do is turn to the website in question and ask for your information to be deleted. However, if the site has a publishing certificate, they have the right to publish the information and do not have to delete it, even if you request it."*

The examples of Sweden and Austria show that at least some Member States fail to perform the proportionality assessment required by Article 85(2) GDPR for the national exemptions/derogations to be legal. Instead, Member States often apply sweeping exceptions/derogations that make the GDPR inapplicable and thereby hollow out the right to the protection of personal data.

4.3. Possible solution

The Commission should undertake a systematic review of Member State law concerning Article 85 GDPR and take appropriate action according to Article 17(1) Treaty of the European Union.

[22] https://www.imy.se/fragor-och-svar/gdpr/ (autotranslated using Google Translate)

We thank you again for giving us the opportunity to meet with you and to share our observations on the enforcement of the GDPR.

We are of course open to organise a follow-up meeting with the Commission regarding the points raised in this letter and any other relevant matter.

Should you need further information, we remain at your disposal under: [redacted] and [redacted]

Kind regards,

noyb team / Max Schrems