



Centre for Information Policy Leadership
— HUNTON ANDREWS KURTH —

CIPL's response to the European Commission's call for evidence on further specifying procedural rules relating to the enforcement of the General Data Protection Regulation

Centre for Information Policy Leadership (CIPL)

23 March 2023

The Centre for Information Policy Leadership¹ (CIPL) welcomes the opportunity to provide input for the European Commission's (EC) call for evidence on *Further specifying procedural rules relating to the enforcement of the General Data Protection Regulation (GDPR)*. This initiative aims to streamline cooperation between national data protection supervisory authorities (SA) when enforcing the GDPR in cross-border cases by harmonising some aspects of the administrative procedures that are applied by data protection SA in these cases.

CIPL took into consideration the issues identified by the EC in the report on the application of the GDPR² as well as the European Data Protection Boards' list³ of GDPR procedural aspects that could benefit from further harmonisation at the EU level when preparing this feedback.

Our response structure follows the EC's suggested high-level policy options to harmonise administrative procedures in cross-border cases. Namely, (1) specify procedural deadlines for cooperation between data protection supervisory authorities on cross-border cases (under Articles 60 and 65 GDPR); (2) provide tools to data protection supervisory authorities to promote cooperation early in the investigation process; (3) clarify the position of complainants in the procedural steps, including the possibility for complainants to make their views known; (4) streamline the way the parties under investigation are heard during the procedure; (5) clarify how information is to confidentially be shared between the investigating data protection supervisory authority and the concerned supervisory authorities at the various stages of the procedure, including in the steps leading to a binding opinion by the EDPB.

¹ CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at <http://www.informationpolicycentre.com/>. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

² 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), available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264>.

³ EDPB Letter to the EU Commission on procedural aspects that could be harmonized at EU level, available at https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-eu-commission-procedural-aspects-could-be_en.

I. INTRODUCTION

CIPL has been at the forefront of GDPR implementation both prior to and after the adoption of the law and has published numerous papers and studies and provided responses to numerous consultations. CIPL has built strong GDPR thought leadership, engaging with regulated entities and regulators alike to drive an approach to enforcement approaches that enable responsible data use while protecting individual's rights.

CIPL believes that any changes, even targeted ones such as this initiative, must be seen in a larger context to ensure the GDPR lives up to its full potential.

The GDPR brought tangible benefits to organisations and individuals and turned privacy into a mainstream business issue beyond just legal and compliance. However, certain elements still need to be addressed or explored further, such as:

1. **GDPR legal bases.** The misperception persists that the GDPR imposes any kind of hierarchy on the available legal bases for processing – it does not; in particular, GDPR does not favour consent over other legal bases. More clarity is also required with respect to the understanding of GDPR's legal basis in the context of other digital legislation, such as the DMA.
2. **Need for greater availability of GDPR accountability tools.** GDPR introduced several accountability-based tools to improve compliance and privacy outcomes, yet certifications and codes of conduct remain rarely available or, where available, impose strict requirements that depart from accountability and risk-based approaches enshrined in the GDPR. Strengthening accountability measures also maximises opportunities for conflict resolution before enforcement actions are contemplated.
3. **Promotion of wider use of BCR.** The current BCR adoption process is burdensome and requires significant time and labour investment. In addition, some of the BCR requirements are stricter than other available transfer mechanisms and lack interoperability and mutual recognition across jurisdictions.
4. **Incentivising the adoption of PET technologies.** Privacy Enhancing Technologies or Privacy Preserving Technologies (PETs or PPTs) are quintessentially privacy by design and hold enormous potential to allow unlocking the full potential of data to the benefit of the digital economy and society at large without compromising privacy.

CIPL intends to provide a more in-depth paper on these issues in advance of the next full GDPR review process.

Importance of the One-Stop Shop

CIPL wants to express its unequivocal support for the GDPR's innovative approach to SA cross-border enforcement, generally referred to as the One Stop Shop (OSS). The OSS is a ground-breaking tool to introduce an integrated and consistent pan-EU enforcement with respect to cross-border processing activities to enable the free flow of data and reinforce the objectives for an EU single market.

The obvious and significant advantage introduced by the OSS is the fact that organisations can rely on one sole interlocutor with respect to enforcement decisions relating to cross-border processing, the Lead Supervisory Authority (LSA), instead of many or potentially all supervisory authorities, depending on the business model. Through this, the LSA has been able to develop a body of knowledge about and expertise in the operations of the relevant organisations. The LSA has been able to leverage their greater understanding of the organisations they supervise to propose appropriate regulatory responses with a view to ensuring compliance for the benefit of individuals.

As processing activities are increasingly performed across multiple countries to serve clients/users in multiple countries or to support multi-country corporate operations, the OSS creates greater legal certainty for all stakeholders and efficiencies in compliance and enforcement.

CIPL strongly supports the OSS as an innovative and essential tool for consistent implementation of the GDPR, providing legal certainty for the benefit of organisations and individuals alike, and any changes to the legal framework should involve careful consideration so as not to undermine the overall functioning of the OSS and, in particular, the special position of the LSA. CIPL has been examining possible avenues for improvement of the system and the development of a common framework for procedural rules for supervisory authority (SA) action since GDPR came into force.⁴

Specific Recommendations on further specifying procedural rules relating to the enforcement of the GDPR

Our recommendations for the development of a common framework for procedural rules for the stages of supervisory action by SAs under Chapter VII of the GDPR are summarised as follows:

- Ensure that regulated organisations have access to all the evidence to be considered in a case
- Ensure that any considered imposition of procedural deadlines takes into account the complexity of the case, safeguards due process, and allows the parties to exercise their procedural rights to the full extent
- Maximising opportunities for resolution before enforcement actions
- Ensure amicable settlements are binding and accompanied by clear rules to streamline the process of reaching a settlement in the OSS procedure
- Ensure confidentiality of the process to be adhered to by all parties to the proceedings throughout the entire cycle of the proceeding

⁴ Please see the following: CIPL Discussion Paper – GDPR Enforcement Cooperation and the One-Stop-Shop – Learning from the First Three Years, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_discussion_paper_-_gdpr_enforcement_cooperation_and_the_one-stop-shop_23_sept_2021.pdf; CIPL Response to the EU Commission’s Public Consultation on the Evaluation of the GDPR, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_eu_commission_consultation_on_gdpr_evaluation_28_april_2020.pdf.

- Embed the right to be heard further into the process, including any Article 65 proceedings in front of the EDPB, including transparency towards the regulated entities with respect to relevant and reasoned objections
- Provide the right to make representations to SAs before formal action is taken
- Avoid overburdening the LSA with administrative requirements in the OSS procedure
- Foster mutual trust between SAs to improve the functioning of the OSS procedure

Taking the above into account, we provide specific comments on the EC's suggested high-level policy options below.

As a general consideration, CIPL invites the EC to provide clarification on the interaction of any proposed legislation regarding streamlining procedural rules that will interact with existing national procedural law.

II. POLICY OPTION 1 – SPECIFY PROCEDURAL DEADLINES FOR COOPERATION BETWEEN DATA PROTECTION SUPERVISORY AUTHORITIES ON CROSS-BORDER CASES (UNDER ARTICLES 60 AND 65 GDPR)

The EDPB notes that the GDPR specifies the number of deadlines applicable to the cooperation procedure, but many of the procedural steps are not subject to any specific deadline. This can, in the EDPB's view, undermine the legal certainty, effectiveness and credibility of the enforcement process. The EDPB further suggests that deadlines could be set on a case-by-case basis for starting the investigation, communicating the information on the case to Concerned Supervisory Authorities (CSA), issuing a draft decision, preparing a revised draft decision after relevant and reasoned objections were sent and adopting a final decision after consensus was reached or triggering the Article 65 GDPR procedure.

CIPL can appreciate that the introduction of specific deadlines in cross-border cases may support a timelier resolution of cases. It is not sufficiently clear whether deadlines are proposed on the parties or on the SAs as well. **However, any introduction of deadlines cannot undermine due process throughout the investigation and must instead provide sufficient time and flexibility for all parties to make submissions as well as for the SA to consider the facts and legal questions of a given matter.**

CIPL submits that any deadlines considered in the context of OSS must take into account that cross-border investigations are, by their nature, complex and may involve a large body of evidence, including thousands of pages of submissions as well as technical material. Parties must be given enough time to exercise their fundamental rights; they must be heard and must have time to reply. The LSA must equally have sufficient time to assess the case and consider all the relevant facts. There is no 'one size fits all' solution, and the rights of the parties must be taken into account when considering any procedural deadlines. The worst outcome would be cases rushed to the decision under artificial deadlines contrary to Article 41 of the Charter of Fundamental rights, which would then more likely than not be challenged in court, ultimately extending the resolution of a matter unnecessarily.

III. POLICY OPTION 2 – PROVIDE TOOLS TO DATA PROTECTION SUPERVISORY AUTHORITIES TO PROMOTE COOPERATION EARLY IN THE INVESTIGATION PROCESS

The EDPB identifies several suggestions in regard to this policy option. Specifically, it calls for clear and harmonised rules on amicable settlements since the majority of Member States do not have a legal framework in place allowing for it.

CIPL specifically supports such settlement provisions providing for commitments; these can foster better compliance since internal oversight systems and processes serve to ensure that such commitments are fully delivered. This is demonstrated in other regulated areas (e.g. competition law, anti-corruption, the EU Consumer Protection Cooperation Network regarding achievements obtained from the acceptance of traders’ commitments) and in other jurisdictions, for example, in the US through FTC consent decrees. Amicable settlements have the potential to enable resource savings at both the national and EDPB level, the potential for much faster outcomes, and faster compliance.

However, the introduction of amicable settlements in the OSS procedure should be accompanied by clear and precise rules. Since the OSS is based on cooperation between LSA and CSA, any rules surrounding amicable settlements must maintain the special position of the LSA or risk diluting the OSS. At the same time, it is critical to ensure that any cooperation requirements do not undermine the purpose of providing a quick and simple solution in the interests of both data subjects and data controllers. Any settlements concluded in the context of OSS must be legally binding.

As a general note, CIPL supports referring consumer complaints to amicable resolutions as a means to resolve non-complex complaints early in the process – this practice should be adopted by all SAs. Similarly, it should be considered whether SAs should require complainants to exhaust company complaints processes first in the interests of an early resolution.

CIPL would like to highlight several other aspects related to promoting cooperation between SAs early in the investigation process. Whereas cooperation between SAs is crucial, it should not undermine the unique position of the LSA and the aim of the OSS. The LSA must be able to independently investigate and handle cross-border cases. While the LSA should take due account of the prior assessment made by the CSA when assessing a particular complaint and share all relevant information about its handling of the case with the CSA, it should be accepted that the LSA may depart from the CSA’s view. Even in cross-border cases where the subject matter of the complaint relates only to an establishment in the local state or affects individuals in that state only. Where the LSA decides to handle the case pursuant to Article 56(4) of the GDPR, the LSA is not bound by the draft decision prepared by the CSA but shall only “take utmost account of that draft.”

CSAs should, in turn, ensure that the LSA is given “enough space” by letting it investigate the case independently in an effective manner so that it can play the “significant role” given to the LSA under the GDPR.

Neither the CSAs nor the EDPB are competent to engage in fact-finding, and in Article 65 dispute resolution procedures, the EDPB is limited to determining whether the CSAs' objections are relevant and reasoned and resolving any dispute related to those objections.

IV. POLICY OPTION 3 – CLARIFY THE POSITION OF COMPLAINANTS IN THE PROCEDURAL STEPS, INCLUDING THE POSSIBILITY FOR COMPLAINANTS TO MAKE THEIR VIEWS KNOWN

According to the EDPB, diverging rules between Member States exist regarding complainants being parties to the procedure, including specific rights conferred on them. Harmonisation of this procedural aspect would help prevent different treatment of complainants between Member States. The EDPB calls to clarify whether the complainant should be actively involved in the procedure, with defined rights, or it could only complain to the SA while not being actively involved in the procedure, as well as to clarify whether the complainant is to be considered as a party to the procedure. Additionally, the EDPB suggest that the representative, as mentioned in Article 80(1) GDPR, when acting on behalf of the data subject, would be entitled to the same status and procedural rights as the complainant who is represented.

CIPL understands the importance of recognising the rights of all parties involved in the OSS procedure. Recognising the complainant as a party can support a more fair and transparent process. This would have to go hand in hand with further defining access rights and providing rules around access to the file.

The inclusion of the complainants as parties to the procedure and access to the file must be accompanied by strong confidentiality requirements and appropriate sanctions for any breach of those confidentiality requirements. Strong confidentiality requirements are necessary as files may contain trade secrets, information covered by IP rights, or information carrying cybersecurity risks. Any access to file procedure would have to also entail clear rules regarding confidentiality designations, rules as to how and with whom confidential information may or may not be shared, as well as effective sanctions to deter parties from disclosing confidential documents pertaining to an ongoing case.

It is crucial that **all** parties respect and adhere to confidentiality obligations to facilitate a fair process without undue influence on the decision-making.

Lastly, the harmonisation of complainants' position in the procedural steps might result in an overall longer OSS procedure; thus, this should be taken into account when considering any procedural deadlines.

V. POLICY OPTION 4 – STREAMLINE THE WAY THE PARTIES UNDER INVESTIGATION ARE HEARD DURING THE PROCEDURE

Currently, parties to the investigation cannot exercise their right to be heard equally in all Member States. The EDPB notes that some Member States allow for the possibility to examine and react to the draft decision, but it is not a general rule. Also, in order to exercise this right effectively, the timing should be clarified, as once the draft decision is shared with CSA, it becomes final. The EDPB suggests specifying the scope of the right to be heard, minimum standards and the timing for documents to be shared and submissions to be taken into account.

CIPL strongly supports strengthening and harmonising the exercise of the right to be heard across all Member States. In addition to providing the right to make representations to SAs before formal action is taken, any proposed rules must ensure that organisations in an investigation have access to all the evidence to be considered in their case. Where member states have different approaches, the right to be heard should cover both legal and factual elements of the case and should also include the possibility of providing written or oral submissions, as appropriate.

Most importantly, CIPL calls for the right to be heard to be extended to any Article 65 proceedings, including in front of the EDPB. Where the EDPB collectively makes a binding decision, the parties must have the right to be heard to alleviate any misinterpretation of the facts and to allow the entity under the investigation to address any new information, change in the scope of the investigation or any other ambiguities. The process must further ensure transparency vis-a-vis the parties with respect to relevant and reasoned objections in the process of OSS.

Ideally, a hearing should take place before the draft decision is prepared and shared with concerned DPAs. Scope, modalities, and timing of hearings should be further clarified with a level of flexibility to determine the format of the hearings, for instance. Summaries of hearings should be provided to all parties, and parties should be given the right to make representations before formal action is taken.

VI. POLICY OPTION 5 – CLARIFY HOW INFORMATION IS TO BE SHARED BETWEEN THE INVESTIGATING DATA PROTECTION SUPERVISORY AUTHORITY AND THE CONCERNED SUPERVISORY AUTHORITIES AT THE VARIOUS STAGES OF THE PROCEDURE, INCLUDING IN THE STEPS LEADING TO A BINDING OPINION BY THE EDPB

The EDPB suggests that the European Commission ought to prescribe the timing, contents and modalities of information sharing between SAs in the course of the OSS procedure. This includes the initial complaint and evidence submitted, relevant official procedural documents adopted by CSA regarding the admissibility of the complaint, all relevant documentation pertaining to investigations carried out by the LSA, including the scoping of the investigation, and a summary of the written submissions by the parties to the national proceedings.

Additionally, the EDPB suggests that LSA should share information about the progress of the case while giving confidentiality assurances.

CIPL agrees that clearly and unambiguously identifying what documents constitute “relevant information” might be beneficial to all the parties. However, it is crucial to consider the LSA’s capacity to prepare and share a large number of procedural documents. Sharing any documents in the context of large-scale cross-border proceedings requires extensive preparation. Thus it is crucial to consider whether increasing the workload of LSAs will work for the benefit of all the parties. In addition, any of the documents shared with CSAs must be coupled with strict confidentiality rules in order to avoid unnecessary information sharing, which can negatively affect the decision-making process. Breaches of confidentiality negatively impact the fairness of the process and can lead to a breakdown in trust in the process and between all involved.

VII. OTHER SUGGESTIONS

Lastly, we highlight that the success of the functioning of the OSS, and overall GDPR enforcement, depends on mutual trust between the SAs. Mutual trust is supported by developing a common understanding of best practices in regulation, exchanging information, rules around the accuracy of sharing information regarding investigations publicly (such as the scope and timelines of the investigation), and shared training. Such increased trust would foster mutual respect between SAs and a common understanding that relevant and reasoned objections should be used by CSAs only in exceptional cases, to be outlined by the EDPB in its guidance, such as serious concerns founded in Article 4(24) GDPR (such as, for instance, in case of high-risk processing) backed by an analysis that goes beyond mere disagreement with the LSA decision.