Position Paper on the Proposed EU Regulation Relating to the Enforcement of the GDPR (Regulation (EU) 2016/679)

Addressing GDPR Enforcement Shortcomings

November 2023

The Computer & Communications Industry Association (CCIA Europe) believes the proposed EU Regulation laying down new procedural rules relating to the enforcement of the General Data Protection Regulation (GDPR) is a welcome opportunity to address shortcomings in GDPR enforcement and improve the handling of cross-border procedures.

As the European Parliament and EU Member States are going to develop their positions in the coming months, CCIA Europe respectfully offers the following recommendations.

I. Harmonising rules for overall enforcement

It is crucial for the GDPR enforcement proposal to establish harmonised rules during the overall process of enforcement – introducing the same requirements before, during, and at the conclusion of all enforcement cases.

Recommendations:

1. Exhaust company's internal processes for handling complaints first
2. Establish clear rules when and how supervisory authorities can contact companies
3. Automatically close cross-border complaints in case of inactivity

---

II. Reinforcing the right to good administration

Fair and impartial handling of cross-border disputes should be given utmost consideration at all stages of the proceedings. This requires adjustments to ensure adequate assessment of objections from concerned supervisory authorities, the strengthening of the right to be heard, and guaranteeing a right to appeal all binding decisions.

Recommendations:

4. Properly assess whether objections really are 'relevant' and 'reasoned'
5. Strengthen right for defendants to be heard at both national and EDPB level
6. Guarantee that EDPB decisions are subject to judicial oversight

---

III. Clarifying the competences and roles of authorities

Cooperation among all parties is crucial for fostering consensus and preventing escalation of cross-border cases. Clearly defining the roles and responsibilities of each authority and party is essential for ensuring streamlined investigations.

Recommendations:

7. Ensure that lead supervisory authorities retain primary competence
8. Mandate cooperation in GDPR cases initiated by authorities other than DPAs

Introduction

The Computer & Communications Industry Association (CCIA Europe), welcomes the overarching goal of improving the enforcement of cross-border data protection cases under Regulation (EU) 2016/679 (GDPR). CCIA Europe Members remain committed to the application of the General Data Protection Regulation (GDPR) and actively collaborate with relevant authorities for enforcement purposes.

Since Regulation (EU) 2016/679 started to apply, some procedural shortcomings in cross-border cases have arisen, undermining the consistent enforcement of the GDPR across the EU and making the regulatory landscape far more complex than it should be.

CCIA believes the proposed Regulation laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679 ("GDPR enforcement proposal" going forward) is an opportunity to address these shortcomings and improve the handling of cross-border procedures. As the European Parliament and the Council are going to develop their respective positions in the coming months, CCIA respectfully offers the following recommendations.

I. Harmonising rules for overall enforcement

It is crucial for the GDPR enforcement proposal to establish harmonised rules during the overall process of enforcement – introducing the same requirements before, during, and at the conclusion of all enforcement cases.

The GDPR enforcement proposal focuses mostly on cross-border proceedings but shies away from addressing other weaknesses that have been identified since the start of the application of the GDPR. In order for enforcement to be actionable and effective, the proposal should consider introducing a number of harmonised rules and procedures for the whole enforcement process, including – at least – the three following best practices.

1. Exhaust company's internal processes for handling complaints first

Since the beginning of the application of Regulation (EU) 2016/679, only a small number of supervisory authorities (SAs) have introduced requirements for complainants to exhaust a company's internal process before a matter can be submitted to them. In light of this, CCIA considers that the GDPR enforcement proposal should strengthen the process set out in Articles 3 and 4 in order to uphold the accountability principle and ensure the lead supervisory authority (LSA) enables all organisations subject to a complaint to first address it using their internal complaint handling mechanism.

Streamlining procedures, particularly in non-complex cases, is key to avoid minor complaints being elevated to the European Data Protection Board (EDPB). This would also help SAs to dedicate their limited resources to the more complex complaints and would ensure alignment of the data protection framework with complaint-handling mechanisms that are applied in other EU sectoral legislation, such as financial and communications services legislation.

2. Establish clear rules when and how supervisory authorities can contact companies

CCIA Europe has observed that some SAs decide to approach companies individually, even though the main establishment of those companies may be elsewhere in Europe. They do so directly without referring to the LSA, arguing that the case is 'local' and falls under their jurisdiction instead of that of the lead authority.

In other cases, we have seen scenarios where SAs reach out directly to companies, arguing that they are entitled to conduct extensive preliminary assessments which they will ultimately hand over to the LSA with all relevant details. Those procedures for detailed preliminary assessments undermine the purpose of the one-stop-shop mechanism and require companies to respond to detailed questions addressed in different languages, even though companies might have previously already answered to their LSA.

In both these scenarios, the lack of clarity defining a local case under Article 56(2) of the GDPR and the extent to which local SAs can conduct preliminary assessments makes it challenging for companies to evaluate or resist these arguments. This puts them in a difficult position vis-à-vis their LSA. In addition, there is always a risk that such practices impede the ability of LSAs and potential concerned supervisory authorities (CSAs) to deal with a case which would normally fall within their jurisdiction.

CCIA believes that the EU co-legislators should clearly define scenarios when "the subject matter relates only to an establishment in [the] Member State [of the SA] or substantially affects data subjects only in its Member State" under Article 56(2) GDPR, and clarify the extent to which SAs are entitled to conduct preliminary assessments for the LSA. The GDPR enforcement proposal should also reiterate SAs' obligation to previously notify the LSA when they seek to approach companies under LSAs' supervision and justify their position, consistently with Article 56(3) GDPR.

In addition, the proposal could mandate the creation of a register of companies' main establishments and their data protection officers (DPOs) to facilitate communication between companies, their LSA, and inquiring SAs in the course of an investigation. Practice shows that several SAs may sometimes directly request companies with a main establishment elsewhere in the EU about compliance with their obligations, without verifying whether the LSA has conducted, or is conducting, a similar assessment.

Further, companies may fail to inform SAs of a data breach, assuming that the notification to the LSA is sufficient and that the LSA will inform other SAs about the breach when necessary. Lack of coordination with the LSA may sometimes be due to the fact that SAs are not aware which LSA they should be reaching out to. Such a register of companies' main establishments and their DPOs, maintained by the EDPB and with input from LSAs (based on controllers and processors' notifications), could help alleviate redundant enquiries and misallocation of SAs' resources.

3. Automatically close cross-border complaints in case of inactivity

Some cross-border complaints can (potentially) remain open indefinitely, long after the company has responded – e.g. over two years after the complaint has been lodged and the competent SA first reached out to the controller. In practice, when SAs initially inquire

directly to the controller / processor with respect to particular conduct or data processing operations, companies may choose to err on the side of caution, and suspend such conduct or processing operation.

While the GDPR enforcement proposal foresees in Article 11(3) the withdrawal of the complaint if the complainant fails to make their views known within the time limit, this should go further and also consider cases to be resolved where SAs fail to provide information about the progress of the case, or where complainants are no longer engaging with the process. In order to ensure a timely resolution of complaints, CCIA recommends introducing a requirement for cases to be automatically closed if the originating SA fails to inform the controller or processor about the progress of the case after the controller's or processor's initial response within a defined period e.g. within four to six months.

In certain cases, this would also help to prevent the suspension of otherwise legal data processing for an indefinite period of time. Such a deadline should only be limited to a duty to inform the controller or processor about the progress of a SA's inquiry, and must be without prejudice to the integrity of the investigation, with regard to the specificity and complexity of each case.

II. Reinforcing the right to good administration

Fair and impartial handling of cross-border disputes should be given utmost consideration at all stages of the proceedings. This requires adjustments to ensure adequate assessment of objections from concerned supervisory authorities, the strengthening of the right to be heard, and guaranteeing a right to appeal all binding decisions.

4. Properly assess whether objections really are 'relevant' and 'reasoned'

In cross-border dispute resolution procedures, relevant and reasoned objections should be properly defined and effectively assessed, introducing the possibility to escalate such objections to the EDPB, who should in turn verify whether they are in fact relevant and reasoned.

Experience with the application of Regulation (EU) 2016/679 has shown the EDPB at times demonstrates little appetite for verifying whether some of the objections by CSAs to an LSA's draft decision are in fact 'relevant' and 'reasoned'. CCIA Europe has observed in some cases acceptance of the CSAs' objections on the basis of a legal and abstract reasoning, without clearly identifying the risks that a draft decision poses nor the impact of the risks posed by the draft decision taken by the LSA.

It appears clear that the dispute resolution procedure will become the main procedural avenue to handle future cross-border cases. In this framework, the GDPR enforcement proposal refers firstly in Article 2(4) to "retained relevant and reasoned objections" and in Article 18 to relevant and reasoned objections, attempting to streamline the requirements to be met by them. However, nowhere is it clearly indicated what constitutes 'relevant' and 'reasoned' objections, and the text makes no reference to the need for an assessment to be conducted by CSAs to demonstrate how reasoned and relevant their objections are.

In addition to the current references in the text, the proposal should include two things. Firstly, a proper definition of what is considered "a relevant and reasoned objection". Secondly, the EDPB should have an obligation to verify whether an objection which the LSA has previously considered as not reasonable or relevant "clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects." This would be consistent with Article 4(24) of the GDPR.

Furthermore, this obligation should apply not only to cross-border cases but also in the context of a cooperation procedure in order to be able to consider which objections are effectively relevant and reasonable.

5. Strengthen right for defendants to be heard at both national and EDPB level

Parties subject to an investigation must necessarily be heard before any decision which negatively affects them is taken. Both the LSA and the EDPB need to take into account the complexity of the case before settling for a deadline that will allow defendants to make their views known.

The right to be heard is a general principle that is enshrined in EU law[1] under the right to good administration, and it must be applied preceding any binding decision. More particularly, when it comes to cross-border proceedings where the EDPB is tasked to settle disputes between the LSA and CSAs, the right to be heard must fully apply to ensure that decisions are fair and the defendants' views are taken into consideration.

More concretely, Article 9 of the draft proposal requires the LSA to prepare a "summary of key issues" before engaging with the parties under investigation. In order to draft such a summary, however, the LSA will likely rely only on the information provided by the complainant, without giving an opportunity to the parties under investigation to provide relevant background information or to correct errors or misunderstandings.

In this context, CCIA recommends introducing a right for the party under investigation to be heard at an earlier stage of the investigation process, in order for the process to be more robust. Local procedures of the Member States should also be taken into account when preparing such a summary of key issues.

Changes to Article 22 should also be introduced to clarify that the parties under investigation have the right to be heard before the EDPB identifies retained relevant and reasoned objections, following the procedure on dispute resolution in Article 22(3).

Moreover, Article 24 of the GDPR enforcement proposal currently foresees that the parties under investigation and / or the complainant shall have one week from the receipt of the statement of reasons to make their views known. This deadline should be two weeks, with the possibility of extension by the EDPB of at least two additional weeks. Indeed, a deadline as brief as the one originally proposed fails to properly take into consideration the potential complexity of the decisions to be taken. Nor does it account for the time needed to draft argumentation. Both are necessary for complainants to effectively exercise their right to be heard.

[1] Article 41(2(a)) of the Charter of Fundamental Rights foresees "the right of every person to be heard, before any individual measure which would affect him or her adversely is taken." while Article 48(2) notes for "respect for the rights of the defence of anyone who has been charged."

Since the entry into application of Regulation (EU) 2016/679, CCIA Europe has observed how the application of the right to be heard varies between Member States. While welcoming the overall goal of harmonising Articles 60 and 65 of the GDPR on cooperation between authorities and dispute resolution, we consider the currently foreseen deadlines in Article 24 of the GDPR enforcement proposal to be too short.

In addition, the EDPB should provide the opportunity for the party subject to an inquiry in a dispute resolution procedure to make its views known on the EDPB's preliminary legal position, before adopting a binding decision. An open channel of communication with the EDPB should be established, thus avoiding the adoption of binding decisions on the basis of an inaccurate or incomplete appreciation of the facts.

To guarantee that a fair and impartial decision is taken, in consistency with Article 41(2) of the Charter of Fundamental Rights, the EDPB should also be required to proactively disclose all relevant materials to the party under investigation. This would include the assessment of facts by the EDPB, its legal characterisation of such facts and new evidence, relevant and reasoned objections, any new evidence on which the party subject to the investigation has not had the opportunity yet to express their views on before, as well as the EDPB's preliminary position.

While acknowledging the fact that the EDPB must adopt decisions within a strict time frame, CCIA strongly believes that the right of a party to a fair and impartial hearing should never be sacrificed. A short time limit may seem efficient, but if it opens the door to legal challenges it will become a source of further delays. In this context, the EDPB should be granted additional resources enabling them to abide by the right to a fair hearing and to do so in a timely manner.

It is also necessary that the GDPR enforcement proposal remains aligned with other established laws that balance the requirement for authorities to act diligently, without undue delay, with the need to ensure fair hearing from all the parties involved before the EDPB adopts a binding decision.

6. Guarantee that EDPB decisions are subject to judicial oversight

When activating the dispute resolution mechanism under Article 65 of Regulation (EU) 2016/679, the proposal should foresee an explicit right for a controller or a processor subject to the investigation to appeal the resulting binding decision that is taken by the EDPB, consistent with the spirit of GDPR and the Charter of Fundamental Rights.

Chapter V of the proposed GDPR Enforcement Regulation is dedicated to dispute resolution. However, while the parties under investigation and / or the complainant are entitled to make their views known in some cases, the proposal doesn't include the possibility to appeal the EDPB's binding decision.

As a result, and considering a recent General Court order,[2] parties subject to an investigation today are deprived of their right to a full judicial review of an EDPB decision affecting them. This is a legal anomaly which EU lawmakers are urged to remedy, consistent with the right to an effective remedy and to a fair trial under Article 47 of the Charter of Fundamental Rights, and Article 6 ECHR.

[2] Order of the General Court of the European Union, dated 7 December 2022, in Case T-709/21, WhatsApp Ireland Ltd v EDPB

Recital 143 GDPR already recognises that: "Any natural or legal person has the right to bring an action for annulment of decisions of the Board before the Court of Justice under the conditions provided for in Article 263 TFEU. [...] Where decisions of the Board are of direct and individual concern to a controller, processor or complainant, the latter may bring an action for annulment against those decisions within two months of their publication on the website of the Board, in accordance with Article 263 TFEU."

A decision taken by the EDPB regarding a specific company in a dispute resolution procedure necessarily affects the company's legal position, given that the LSA cannot depart from the EDPB's findings in its final decision. CCIA considers that the dispute resolution procedure must uphold the fundamental right to an effective remedy and a fair trial for the investigated party.

While the LSA's final decision, which contains the legal substantive elements of an EDPB decision, may be subject to an appeal before a national court, such national court is not allowed to declare EU acts (i.e. an EDPB decision in this case) invalid. At best it can refer the matter in case of doubt to the Court of Justice of the European Union (CJEU).

However, even with referrals, the gap in judicial review persists, insofar as the CJEU lacks the power to review all factual and legal matters pertinent to the dispute before it. This would include omissions of factual elements, such as potential procedural violations identified during the course of a dispute resolution procedure.

It is essential in this context to ensure that the EDPB is accountable for the impact that its decisions might have. For this reason, anyone affected by an EDPB decision that regards them needs to have a meaningful right to judicial redress. Furthermore, it is only with an effective right to redress that the European Union can expect third countries to observe this right in order to be recognised as providing a level of protection which is "essentially equivalent" to the European Union's.

III. Clarifying the competences and roles of authorities

Cooperation among all parties is crucial for fostering consensus and preventing escalation of cross-border cases. Clearly defining the roles and responsibilities of each authority and party is essential for streamlined investigations.

7. Ensure that lead supervisory authorities retain primary competence

New rules on enforcement must ensure that the LSAs maintain their competence as principal investigator in order to ensure efficient investigations and allow controllers to have one single interlocutor in cross-border cases.

Regulation (EU) 2016/679 established the concept of lead supervisory authorities and defined their powers as a way to facilitate the implementation and enforcement of the Regulation. This is also in line with efforts to minimise regulatory burden and cost for organisations that operate in more than one EU Member State. The proposed rules on cross-border enforcement cases should not seek to undermine this important concept, which guarantees the efficient handling of complaints, facilitates exchanges between

relevant authorities and the parties under investigation, and avoids the role of the lead supervisory authorities inadvertently being undermined.

While we welcome the goal of the proposal of ensuring that supervisory authorities cooperate early on, while ensuring that the EDPB only seeks to resolve disagreements without engaging in further fact finding, it should be clear that only LSAs have an exclusive competence to carry out the complex factual and legal assessments at hand, and determine appropriate sanctions.

The proposed language in Articles 10 and 18(1) risks however undermining the authority and sole discretion of the LSA, while Article 11(5) enables another authority to prepare the draft decision under Article 60 of Regulation (EU) 2016/679. This risks severely undermining the one-stop-shop mechanism and could result in further delays in the process of adopting a binding decision.

What is more, it should not be possible for relevant and reasoned objections to change the scope of the allegations, nor to change the nature of the allegations raised. Regulation (EU) 2016/679 is clear about LSAs' competences and the GDPR enforcement proposal should not grant the power to determine the relevant facts and calculate fines to authorities other than the lead supervisory authorities.

8. Mandate cooperation in GDPR cases initiated by authorities other than DPAs

Effective rules for good faith cooperation should apply when authorities other than data protection supervisory authorities examine inconsistencies of a company's practices with the GDPR.

A recent CJEU judgement[3] has opened the door for authorities other than data protection SAs to examine the GDPR compliance of a company's practices. The GDPR enforcement proposal, however, does not foresee any mechanism for sincere and effective cooperation rules in these cases. This is much needed in order to guarantee the involvement of data protection authorities in these cases and ensure they are informed in an effective and satisfactory manner.

In those cases, checks and balances must be introduced in Article 7 of the proposal to ensure good faith and sincere cooperation and avoid multiple parallel investigations (both among authorities and among Member States), and to safeguard against possible violations of the principle of *ne bis in idem.* New requirements that guarantee such principles of sincere and effective cooperation shall include the following.

- Where there is (or there might be) an on-going procedure led by the LSA, or where the LSA has already taken a decision regarding the same conduct, the national investigating authority must:
    - Consult the LSA in case the investigating authority has doubts as to whether the conduct at hand may already be subject to an investigation initiated by the LSA and justify why this data protection assessment is required to assess the relevant matter under the competence of the national investigating authority;

[3] Case C-252/21, Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social), 4 July 2023

  - Await the outcome of the LSA's investigation before commencing its own assessment on the matter under its own legal remit;
  - Refrain from deviating from the interpretation of the LSA if the latter has already ruled on the compliance of a company's conduct with the same provision;
  - Comply with a decision adopted by that authority concerning the same conduct.

- Where it is clear that the LSA has not launched any investigation or proceedings for the same conduct, the national investigating authority must:
  - Inform the LSA early on about the need to have the LSA examine compliance of a company's conduct with GDPR;
  - Request from the LSA a binding opinion on the investigating authority's draft decision, only insofar as it concerns preliminary findings of a GDPR violation.

Omitting these provisions would only further exacerbate the recent trend of fragmentation in GDPR enforcement, which is precisely what the proposal aims at addressing. Furthermore, the risk of a company's liability exposure would also increase beyond the 4% global annual turnover maximum fine currently set in the GDPR.

Conclusion

CCIA believes that the proposed new rules on GDPR enforcement hold the potential to complement the existing data protection framework and address some of the shortcomings identified during the implementation of Regulation (EU) 2016/679.

Overall, the Association believes that regulatory harmonisation and consistency, building on the GDPR foundations, should drive the discussions on this proposal. We are strongly committed to assisting EU lawmakers in this endeavour.

About CCIA Europe

The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross section of computer, communications, and internet industry firms.

As an advocate for a thriving European digital economy, CCIA Europe has been actively contributing to EU policy making since 2009.

CCIA's Brussels-based team seeks to improve understanding of our industry and share the tech sector's collective expertise, with a view to fostering balanced and well-informed policy making in Europe.

Visit ccianet.org/hub/europe/ or x.com/CCIAeurope to learn more.