Ecommerce Europe reply to the Call for Evidence on further specifying procedural rules relating to the enforcement of the General Data Protection Regulation

1. Introduction

The aim of the initiative on 'further specifying procedural rules relating to the enforcement of the General Data Protection Regulation (GDPR)' is to streamline cooperation between national data protection supervisory authorities when enforcing the GDPR in cross-border cases. To fulfil this objective, the initiative proposes to harmonise certain aspects of the administrative procedures applied by the relevant data protection supervisory authorities in such cases. Ecommerce Europe generally perceives the European Commission's initiative to refine the existing procedural rules on GDPR enforcement positively, as current procedural differences, due to lack of harmonisation across the EU Member States, might be highly impactful for the parties involved under investigation – including businesses. However, Ecommerce Europe also encourages the European Commission to be mindful of ensuring that the One-Stop-Shop (OSS) mechanism, introduced under Article 56 GDPR, is maintained and strengthened to ensure a level playing field and legal certainty for businesses operating across different EU Member States; that the rights of the parties involved in the investigation procedure, including in particular the right to be heard, also before the EDPB, is ensured; as well as that the right to due judicial process is not constrained by fixed and arbitrary procedural deadlines that do not take into account the specificity and complexity of the subject matter in question. Finally, we find it relevant to emphasise that since a general evaluation of the GDPR is expected next year, we argue that the European Commission should refrain from reopening the GDPR, and rather focus its efforts on a targeted proposal only addressing the relevant procedural aspects of enforcement under the GDPR. As such, Ecommerce Europe urges the Commission to ensure that the planned initiative focuses only on the cooperation between national data protection authorities and does not contain provisions that will affect the data subjects, controllers, or processors. As this initiative generally is perceived to respond to the European Data Protection Board's (EDPB or 'the Board') letter of recommendations of 10 October 2022, which identifies procedural aspects of the cooperation between Supervisory Authorities (SAs) in cross-border cases that calls for further harmonisation at EU level, we will address key concerns related to the proposals of the EDPB in the following paragraphs.

2. Scope of the initiative

In its Call for Evidence on 'further specifying procedural rules on the enforcement of the GDPR', the European Commission refers to Article 16 of the Treaty on the Functioning of the European Union (TFEU) as its legal basis for the upcoming legislative initiative. Article 16 (TFEU) lays down rules on the ordinary legislative procedure, under which the European Commission may introduce regulatory proposals, including within the area of data protection, processing of personal data and the free movement of such data. However, since the Commission has not yet issued any information on what type of legislative initiative they intend to propose, i.e. whether they will revise the existing GDPR, if they will present a completely new regulatory proposal, or if they will make use of implementing acts, Ecommerce Europe calls for further information on this matter and clarification of the legal basis behind the initiative to ensure that the scope

of the proposal does not go beyond the competences of the Commission, depending on which legislative approach the Commission decides to pursue. For instance, Article 61(9) GDPR empowers the Commission to adopt implementing acts to specify the format and procedures for mutual assistance between Supervisory Authorities (SAs), as well as Article 67 GDPR grants the Commission the power to adopt implementing acts on the arrangements for the exchange of information between SAs, and between SAs and the European Data Protection Board (EDPB). Aside from these referred articles, the Commission has no further power to adopt implementing or delegated acts on procedural aspects of enforcement of the legislation. As such, Ecommerce Europe presumes that any regulatory proposals that go beyond this framework could only be established through the ordinary legislative procedure under Article 16 (TFEU).

3. General enhancement of the One-Stop-Shop mechanism under the GDPR

The One-Stop-Shop (OSS) mechanism, introduced by Article 56 GDPR, allows companies carrying out cross-border personal data processing to engage with one Lead Supervisory Authority (LSA), rather than the relevant Supervisory Authority of each EU member state, thus ensuring legal certainty for businesses and generally making it easier for companies to operate in different EU Member States. A consistent and harmonised application of the GDPR remains essential, and therefore, Ecommerce Europe strongly supports the preservation and strengthening of this mechanism, and notes that the European Commission's new legislative initiative on GDPR enforcement should only reinforce procedural issues, which will enable more effective cooperation between authorities on cross-border issues. As such, we argue against expanding the ability of the wider community of Data Protection Authorities (DPAs) to review and comment upon factual findings, draft decisions and ultimate sanctions recommend to the lead DPA during the course of the investigation. Likewise, we also argue that the role of the EDPB and the cooperation mechanism should be the exception and not function as a general appeal instance for legitimate decisions taken by the lead DPA. Rather, we suggest the Commission to look into ways of simplifying the cooperation mechanism.

One of the prerequisites to achieve harmonised enforcement of the GDPR in cross-border cases is for national DPAs to have a common understanding and interpretation of the EU data protection law. Currently, such harmonised interpretation is lacking. Based on observed activity of the local European DPA offices, Ecommerce Europe notes that there are visible differences in the interpretation and application of the GDPR across different EU Member States, leading to forum shopping among complainants. This brings about a number of competitive disadvantages for companies based in Member States that interpret and apply the enforcement provisions under the GDPR more strictly compared to other Member States. A concrete example of such differences is, for instance, that there is a general expectation within the German market that e-commerce platforms should always make it possible to make a purchase without registration of the customer. This is, however, not a commonly shared position across all Member States. If comparing to the case of Poland, an e-commerce platform registered in Poland, offering e-shopping services to German clients, can rely on the Polish DPA's requirements, which differ from those of the German DPA. As such, Ecommerce Europe argues that one of the persisting issues of the current OSS mechanism is that it has not yet resulted in a level playing field of enforcement. Yet, abolishing the current OSS mechanism, to instead introduce a multiple-shops formula, would be more conducive to deepening the differences between EU Member States rather than supporting further harmonisation. It would also significantly reduce the predictability of the processes since these local differences must then be addressed by companies carrying out cross-border personal data processing. More specifically, introducing a multiple-stop mechanism, instead of the OSS mechanism currently in place, would open Pandora's box in the sense that businesses would have to deal with the complex issue of foreign law application and obligations for companies operating cross-border to monitor the national laws of 27 EU Member States, as well as to follow 27 legal interpretations of the GDPR. This would lead to a very complex legal landscape for businesses to navigate

in. For multi-country platforms, where it is not possible to limit the potential range of clients, as well as businesses operating across the Union more generally speaking, we therefore do not see any other solution than to have one single supervisory authority. Another advantage of the OSS mechanism is also the possibility of cooperation with local authorities that are believed to have the best knowledge on the interplay between the GDPR and specific local provisions, such as specific national contexts, legal traditions etc. This is especially important seeing that provisions under the GDPR, such as Article 6, often refer to national provisions which are often supervised by local offices or authorities.

Moreover, although the EDPB is tasked with "providing general guidance (including guidelines, recommendations and best practices) to clarify the law and to promote a common understanding of EU data protection laws", it has been observed on a number of occasions that national DPAs are departing from such guidelines when enforcing the law. For example, in its latest annual report, the DPA of Baden-Württemberg (Germany) explicitly disagreed with the EDPB's position on the concept of international data transfers, specifically if a controller's employee working from a third country is contrary to performing a data transfer. Other examples include divergent national interpretations of the concept of legitimate interests, requirements related to cookies and tracking technologies etc. Where such harmonised interpretation is not ensured, it is unlikely that unified procedural rules alone will bring about the necessary level of legal certainty to the parties of the proceedings and sufficiently protect the rights of the data subjects. Therefore, Ecommerce Europe strongly recommends including this overarching challenge of harmonisation in the European Commission's problem statement and to advance a regulatory amendment to ensure that the guidelines and position of the EDPB take precedence over the national interpretation of the same provisions by the DPAs.

4. Rights and definition of parties involved in the investigation procedure

In its letter, the EDPB recognises that procedural rights ascribed to the parties of an investigation differ between the EU Member States. Therefore, the Board suggests enhancing harmonisation and ensure a more uniform application of the GDPR by establishing a list of procedural rights to which the parties involved are entitled, regardless of which member state the case takes place in. It is further noted that such increased harmonisation of the parties' procedural rights at national level will also be beneficial in cross-border cases requiring dispute resolution by the EDPB in accordance with Article 65(1)(a) GDPR. Ecommerce Europe would, however, argue that while the GDPR already provides for a comprehensively harmonised and conclusive regulatory framework, enabling data subjects to pursue public enforcement of their rights via independent SAs pursuant to Article 51(ff) GDPR, which already are empowered with specified competences and tasks, the GDPR's enforcement framework lacks harmonisation. Moreover, the principle of the OSS mechanism, under which the LSA of the controller's main establishment is the sole point of contact competent for the controller's cross-border data processing operations (Article 56(1) GDPR), ensures that the regulatory enforcement system is cooperative and consistent. In relation to this OSS mechanism, the LSA shall, pursuant to Article 63(ff) GDPR, cooperate sincerely and effectively with other SAs. This harmonised regulatory framework, including the substantive provisions of the GDPR, seeks to fulfil the equally important objectives of the Regulation, namely, to ensure the same high level data protection of natural persons and the removal of barriers to personal data flows within the EU, as well as ensuring an adequate balance of the data subject's and controller's fundamental rights, and where applicable, those of third parties in the Union at the administrative and procedural level. Based on this perception of the GDPR's existing enforcement procedures, Ecommerce Europe trusts that the European Commission's upcoming proposal(s) will not jeopardise the already balanced system in place for the benefit of both data subjects and controllers.

4.1 Complainants as parties to the procedure

In line with the rights of the parties involved, some of the proposals put forward by the EDPB request further harmonisation and clarification of the complainant. Particularly, the Board recalls that the GDPR enforcement would benefit from clarification on whether complainants, and their potential representatives, shall be regarded as parties to the procedure, including having an active role in the procedure with specific rights conferred upon them. Currently, the status of complainants is perceived differently across Member States, with some Member States regarding complainants as parties to the procedure, while others do not. Ecommerce Europe would be worried that such harmonisation proposals from the EDPB could potentially increase the powers of the complaining party (e.g., privacy interest groups and aggrieved individuals) by allowing it to review and comment on case files and participate directly in the proceedings as a party. The European DPAs bear the responsibility of the protection and adjudication of data privacy interests, as well as the protection of fundamental rights, in the Union. As such, inspection procedures of the DPAs should be understood as being more inquisitorial of nature rather than adversarial. Ecommerce Europe therefore calls on the Commission to remain prudent about letting complainants into the investigation fold, by providing them with the status of a party in the investigation, as such introduction of potentially adversarial elements into an essentially inquisitorial process could impact the equilibrium of investigation procedures, and result in a violation of the equality of arms principle and right of defence principles.

4.2 Right to be heard

According to the EDBP, the upcoming initiative on GDPR enforcement procedures should also ensure further harmonisation on the scope, modalities and timing of the right to be heard of parties. Currently, the scope of the right to be heard in the context of an SA's investigation varies depending on national rules. As such, some Member States only allow parties under investigation to provide submissions on factual points. Ecommerce Europe therefore supports any proposals that would increase the powers of the respondent to be heard during judicial proceedings. More specifically, we firmly argue that to give full effect to the right to be heard, as laid down in Article 41 of the Charter of Fundamental Rights of the European Union, it is vital that this right entails both factual and legal elements raised in the investigation, and that it provides the parties with the possibility of making written and/or oral submissions, as appropriate.

Furthermore, we understand that the EDPB's recommendation regarding parties' right to be heard in the context of cross-border investigation cases is limited to hearings before the SAs. Ecommerce Europe believes that this right should be extended to include the EDPB in cross-border cases, when disputes are being resolved between different DPAs and when the cooperation mechanism, pursuant to Article 60(ff) GDPR, has been triggered. More specifically, we are concerned that the insistence that the right to be heard should only be offered before the SAs undermines the importance of the right to be heard before the EDPB. In cross-border investigations, where the EDPB is empowered to resolve disputes between SAs, it is inconceivable that the party under investigation are not afforded the possibility of being heard directly by the EDPB.

The experience of some members of Ecommerce Europe has been that in certain inquiries, the absence of a right to be heard before the EDPB can lead to it adopting binding decisions based on inaccurate or incomplete understandings of the facts, which could have been remedied via explanation by the parties. More specifically, parties that are subject to investigations can make submissions to the LSA in respect of the other SA's objections before the LSA finalises its draft decision. However, parties are stripped of the opportunity to comment on the LSA's final draft decision before it being submitted to the EDPB, and they also have no option to comment on the EDPB's analysis and assessment of those objections. It is frequently the case that the EDPB adopts an entirely new position on the applicable legal principles, which has never

been presented to the parties and to which the parties have not been offered any right to be heard. As such, Ecommerce Europe argues that the EDPB should grant the party under investigation a right to be heard, in both written and oral communication, as well as an opportunity to respond to the positions that the EDPB intends to adopt in the procedure leading to its binding decision. This is necessary because decisions adopted by the EDPB can lead to significant administrative fines and/or detrimental effects on the position and activities of the party under investigation. An oral hearing would allow the investigated party to eliminate potential factual uncertainties and inaccuracies, as well as address any concerns raised by the EDPB in respect of the legal position adopted by the party under investigation. This would, however, require that the Board proactively discloses case material (such as facts, legal characterisations of those facts, and evidence on which the EDPB relies), together with its preliminary position, to the party subject to investigation. In line with this, it should also be noted that while the EDPB is required to base its decision on facts as found by the LSA, the right to be head before the EDPB must apply to both the legal characterisation of those facts by the EDPB and the legal position the EDPB intends to adopt. As such, the investigated party's right to be heard directly by the EDPB in proceedings pursuant to Article 65, should take place ahead of the EDPB adopting its decision. In practice, this means that the party under investigation should have the right to be obtain access to the provisional views of the EDPB and be offered the possibility to respond to these views prior to the Board finalising its decision. Overall, Ecommerce Europe is of the understanding that the harmonisation of rules on the right to be heard before SAs would be ineffective, if not complemented by a systematic right to be heard before the EDPB. Underlining our arguments, we also believe that the merger control procedures under Regulation (EC) 139/2004 demonstrates that it is indeed possible to reconcile the need for authorities to act swiftly and diligently with the need to provide the concerned parties (in this case controllers) with effective rights to a fair hearing within short but sufficient timeframes.

Finally, Ecommerce Europe strongly encourages the European Commission to also strengthen the right to be heard by harmonising rules on the involvement in the proceedings of third parties, beyond the complainant and a legal entity directly subjected to the investigation (e.g., a company against which the complaint has been raised). Such need for harmonisation rules may arise where a matter under investigation involves a set of data processing operations carried out by the legal entity and other (joint) data controllers or data processors, and, as such, the informed understanding of the (technical) set-up of such processing operations requires third parties to provide additional factual information, as well as responsibility for the implementation of data privacy controls, due to the statutory and/or contractual set-up, is distributed among the parties. Various Google Analytics cases decided in 2022 by different DPAs constitutes examples of such scenario, as the website publishers, alongside Google as a data processor, were involved in the legal proceedings of these cases.

4.3 Position of complainants in the procedural steps: Access to file and confidentiality

The EDPB also suggests to European Commission to further specify the right of the parties to access documentation of the proceedings, calling on clarification on what constitutes the minimum scope of the file, as well as the scope of the access that should be granted to the parties involved. Ecommerce Europe does not object to complainants being appropriately involved in the procedure, as we, in principle, agree that it would be useful to harmonise rules on what constitutes the minimum scope of the file, i.e. the required type of documents to be included. With that being said, Ecommerce Europe does have reservations regarding the scope of potential access. In light of the risk of (high-profile) complainants leaking confidential information of on-going investigations to the media, we firmly argue that no procedural rules should be adopted in this respect without also laying down stringent accompanying rules on confidentiality, as well as appropriate sanctions for any breaches of such confidentiality obligations. Ecommerce Europe considers it

essential to avoid leaks that could undermine the integrity of the decision-making process based on the external pressure that such leaks can cause. In line with this, we further note that the EDPB also calls for specifying rules on confidentiality. Given the sensitivity of cross-border investigations, it is of vital importance that recipients of information received as part of the access to the file are prohibited by law from disclosing any such information to anyone who is not a party to the proceedings, as well as these should be prohibited from using the information they obtain for any purpose other than the conduct of the inquiry. Again, Ecommerce Europe strongly considers that any failure to comply with such prohibition should be met with deterrent sanctions.

5. Procedural deadlines

Within the current legal enforcement framework of the GDPR, a number of procedural steps in the process of case handling (both at national level and in relation to cross-border cases) are not subject to any deadlines. Ecommerce Europe therefore acknowledges that the EDPB is concerned that the absence of procedural deadlines may cause undue delay and/or disparity in the finalisation of cases. The EDPB suggests the introduction of deadlines for a number of procedural steps to avoid undermining the credibility of enforcement and to contribute alleviating public concern from complainants that cases are being handled too slowly. More concretely, this would entail specified deadlines e.g., to start an investigation; to issue a draft decision; or to prepare a revised draft decision after relevant and reasoned objections have been submitted. The EDPB further recognises that such deadlines must take into account the specificity and complexity of each case. Where not able to meet the established procedural deadlines, the LSA would have to provide justification and would face consequences for its failure to comply with these.

Ecommerce Europe would like to stress that the time required to complete each procedural step in an investigation highly depends on the complexity of the subject matter of the inquiry in question. The initiation of investigations, the issuing of a draft decision, and preparation of a revised draft decision are all complex procedural steps that must be carefully made by the relevant authorities, and these steps should therefore not be constrained by artificial and arbitrary deadlines. We are concerned that providing for fixed deadlines for procedural steps which apply to all inquiries without discrimination, and without consideration of the complexity of the subject matter, would likely operate to the detriment of the party under investigation and undermine the fair, properly reasoned, efficient, and consistent application of the GDPR. In this regard, Ecommerce Europe also deems it necessary to underline that the exercise by the SAs of their powers must be “subject to appropriate safeguards, including […] due process set out in Union and Member State law in accordance with the Charter” (Article 58(4) GDPR), as is also the exercise by the SAs of their power to impose administrative fines (Article 83(8) GDPR). Moreover, we question how such procedural deadlines could be compatible with a case-by-case analysis taking into account the specificity and complexity of the given investigation and the procedural safeguards provided for under the applicable national law, which must be respected in accordance with Articles 58(4) and 83(8) of the GDPR. We strongly believe that arbitrary procedural deadlines will result in rushed decisions and, as such, will also be more likely to result in decisions being challenged by the parties under investigation and subsequently overturned by the courts. Furthermore, Ecommerce Europe also calls for further clarification about how the fundamental rights of the party subject to investigation could be adequately respected where such arbitrary deadlines apply to all inquiries, regardless of the surrounding circumstances. We note that the EDPB has expressed concern and frustration over the fixed deadlines imposed on the Board itself under the Article 65 (GDPR) process, and we find it incomprehensible why the EDPB would seek to impose such deadlines on the SAs. Finally, if concerns persist about the ability of the SAs to progress investigations in a timely manner, while simultaneously ensuring due judicial process for the subject of the inquiry, this should be addressed by ensuring that the SAs have the necessary human and financial resources to perform their tasks in a timely

manner – not by restricting the procedural safeguards to which controllers are entitled. This is particularly so in light of the magnitude of the administrative fines which might be imposed under the enforcement of the GDPR.

6. Complaint handling through amicable settlements

Among its suggestions for refining procedural rules relating to GDPR enforcement, the EDPB also calls for clarification and harmonisation of provisions on resolving complaints through amicable settlements or other non-contentious ways, as well as it requests clarification of the applicability of Article 60 (cooperation under the OSS mechanism) in case of amicable settlements. Generally, Ecommerce Europe believes that an outcome-focused approach should place judicial proceedings and related administrative sanctions as a measure of last resort, and that DPAs should instead make increasingly use of the wider range of measures available under the GDPR, such as formal warnings or correction notices. Moreover, we argue that the Commission should support the proposal put forward by the EDPB to explicitly authorise DPAs to enter into amicable settlements in non-contentious ways. Regarding severe cases creating serious harm for individuals, and where sanctions are appropriate, the EDPB should develop and publish a clear, predictable, consistent and proportionate model for calculating actual fines, which takes into consideration mitigating factors and which are distinct from statutory maximums.

Regarding amicable settlements, the Board also proposes the need to clarify that such settlements achieved in the context of the OSS on a specific case also requires cooperation on the legal questions behind the individual case – either by demonstrating it as an isolated case or by explaining what follow-up actions are intended to be taken in view of the breach of GDPR provisions by the controller. Although generally being in favour of clarifying the framework for amicable settlements, especially in EU Member States which currently do not have a legal framework for this, any such initiative should ensure that settlements are not burdened by too far-reaching coordination obligations. Otherwise, we fear that this could unreasonably deprive the LSA of its prerogatives and could have the effect of turning settlements, intended to be quick and simple resolution mechanisms in the interests of both data subjects and controllers, into long and complex legal processes. Furthermore, it could also discourage the use of amicable settlement of disputes, which we believe would be strictly contrary to the objectives of the GDPR. Ecommerce Europe would therefore like to stress the importance of not distorting the enforcement system in cross-border cases established by the GDPR through procedural rules. While we recognise the objective of ensuring efficient and harmonious enforcement between SAs in such cases, it is at the same time vital to preserve the LSA's independence and its prerogatives as established by the GDPR. Finally, with regards to amicable settlements, Ecommerce Europe calls on the Commission to specify confidentiality and non-disclosure guarantees, as we argue that this would provide impetus for parties to conclude such agreements. More specifically, parties will be more incentivised to resolve disputes by means of amicable settlements, if there are adequate assurances in place specifying that details of such settlements will not be publicly disclosed. This will require harmonisation of the way in which DPAs publish information on enforcement actions, as, for instance, some DPAs issue press releases specifying the names of the companies under investigation, whereas other DPAs do not.

7. Investigative powers

With regard to investigative powers under the GDPR, we understand that the EDPB recommends the European Commission to provide uniform and consistent rules for identifying cases where further investigation is not warranted, as this would contribute to mitigating legal uncertainty and harmonise practices across the Union. Ecommerce Europe, however, believes that such rules would likely affect the LSA's independence and margin of discretion to assess the elements of each case. As such, we believe

that the Commission should refrain from proposing such rules in its upcoming legislative initiative, or at the very least give due consideration to the LSA's margin of discretion and powers.

8. Cooperation procedure under Article 60 GDPR

The EDPB, in its letter of recommendations to the European Commission, addresses the need to harmonise the cooperation procedure under Article 60 GDPR, obliging the LSA to cooperate and share information with the concerned SAs also before the draft decision stage. As such, the Board suggests laying down rules on further clarification and harmonisation of the timing, content and modalities of information sharing and cooperation in the context of cross-border cases to an extent that Ecommerce Europe finds too strict. We are concerned that such rules would only contribute to increasing the already significant pressure on LSAs, as these, combined with the numerous deadlines sought to be imposed on (L)SAs by the EDPB, will have a constraining and counterproductive effect on the workload of the supervisory authority in question. Finally, we further stress that any such rules would also have to address the necessity to preserve the confidentiality of inquiry documents, as to preserve the integrity of the decision-making process.

9. Final general comments and observations on GDPR enforcement

Following our concerns related to the EDPB's proposals for specifying procedural rules for enforcement of the GDPR, as addressed above, we will now provide some more general comments and observations on aspects of the current GDPR enforcement regime. Firstly, Ecommerce Europe calls for further clarification of what is to be understood as a "local case" under Article 56(2) GDPR. Despite the OSS mechanism in place, granting power of enforcement in cross-border cases to the LSA, in accordance with Article 56(1) GDPR, we sometimes experience that other DPAs approach companies on the basis of Article 56(2) GDPR. More specifically, the respective authorities argue that the case in question is considered as "local" and that they would be competent for such case, thus derogating from the rule on the LSA under Article 56(1) GDPR. For companies, the arguments put forward by authorities in such situations can be incredibly hard to assess and as a result of this, it might also be difficult to push back given the lack of very specific rules on this matter. Against this background, Ecommerce Europe would find it helpful to have more clarity on what the underlined wording means under Article 56(2) GDPR: "By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State."

Moreover, Ecommerce Europe also calls for clearer rules and obligations for DPAs when cooperating with other regulators. While we recognise that the upcoming initiative currently discussed only deals with cooperation between privacy regulators, companies sometimes find themselves stuck in between different compliance expectations and requirements coming from different regulators. To avoid legal uncertainty, it would therefore be helpful in these cases to have clearer rules and obligations for privacy regulators to also discuss and align their positions with other authorities, such as tax authorities, financial authorities (in the anti-money laundering area) etc., when it comes to legal enforcement against companies.

We would, in addition, encourage the European Commission to also focus its efforts on constructive regulatory dialogue. The GDPR is a principles-based legislation, whose practical application is highly dependent upon specific facts and circumstances. As such, we believe that constructive dialogue between regulators and companies should be encouraged to help regulators better understand the technical and operational impacts of the GDPR before taking any formal action of enforcement. This could, for instance, include the creation of industry stakeholder groups consulted by regulators and privacy sandboxes, enabling businesses to access data about its users without compromising the privacy of these.

Finally, in its Call for Evidence, the European Commission has decided to not produce an impact assessment, as “the initiative will not affect the rights of data subjects, the obligations of data controllers and processors, or the lawful grounds for processing personal data as set out by the GDPR”. Ecommerce Europe therefore urges the Commissions to ensure that the planned initiative focuses only on the cooperation between national data protection authorities and does not contain provisions that will affect the data subjects, controllers, or processors.