24 September 2021

CIPL Discussion Paper
GDPR Enforcement Cooperation and the One-Stop-Shop
Learning from the First Three Years

Methodology and Summary of Recommendations

The One-Stop-Shop mechanism (OSS), is essential to support the consistent implementation of the GDPR in order to achieve the EU single market. The OSS brings important benefits to individuals, organisations and Supervisory Authorities (SAs). However, the OSS is facing a growing amount of criticism and risks being undermined. Its challenges should now be discussed and addressed, with all those involved, working together to support the OSS.

CIPL started working on the OSS at the end of 2020. At this time, CIPL's objective was to issue a comprehensive and wide-ranging discussion paper based on feedback from members with global headquarters in the EU as well as outside of the EU, providing background information and spotting the main issues. The project was based on the premise that the Lead Supervisory Authority (LSA) should have a prominent and strategic role in the OSS mechanism while enabling meaningful involvement of the Concerned Supervisory authorities (CSAs). The initial paper was intended to serve as a basis for wider discussions on several aspects of the OSS with those who have been affected by OSS decisions, SAs who are working in the OSS and a range of academics and commentators, before recommendations would be made. There have been, however, a number of key recent developments that have impacted the original project:

- **adoption of several EDPB guidelines on the working of the OSS;[1]**
- **adoption of EDPB documents on GDPR cooperation and enforcement;[2]**
- **first EDPB binding decisions;[3] and**
- **CJUE decision clarifying the OSS.[4]**

As a consequence, the initial wide-ranging paper was turned into a narrower discussion paper (Paper) that not only identifies the challenges, defines CIPL's position on some of these points, but also proposes possible solutions to improve the OSS mechanism, taking into account the EDPB's work as well as CJUE decisions.

---

[1] See Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679; Guidelines 03/2021 on the application of Article 65(1)(a) GDPR; Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities.

[2] See EDPB Document on Terms of Reference of the EDPB Support Pool of Experts; EDPB Document on Coordinated Enforcement Framework under Regulation 2016/679.

[3] Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR; Urgent Binding Decision 01/2021 on the request under Article 66(2) GDPR from the Hamburg (German) Supervisory Authority for ordering the adoption of final measures regarding Facebook Ireland Limited; Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR.

[4] See Facebook v Gegevensbeschermingsautoriteit; Case C-645/19.

CIPL believes a strong effort should be made at the European level and among SAs to address the OSS challenges. In order to achieve this, CIPL recommends the EDPB to:

- **continue to work further to foster respect, mutual recognition, sharing and understanding of the regulatory approaches, processes and decision-making capacity of other Member States;**

- **take inspiration from areas where approaches to build a common understanding of problems, procedures and regulatory techniques have successfully developed trust and improved working relationships;**

- **encourage the creation of a common framework for procedural rules for the stages of supervisory action under Chapter VII of the GDPR, including rules on transparency and the right to be heard;**

- **continue to promote the application of the OSS in the e-Privacy Regulation and other digital areas to ensure consistent enforcement and reduce the risk of double jeopardy;**

- **foster exchanges between SAs regarding different regulatory approaches, the compliance effects they deliver, and methods of encouraging behavioural changes focused on desired outcomes;**

- **continue to ensure that "relevant and reasoned objections" and mutual assistance and joint operation procedures should only be used in limited cases of serious concern to further promote SAs' self-restraint;**

- **consider enabling organisations to validate their main establishment and set up a voluntary register;**

- **adopt guidelines on how corrective measures should apply, including a clear and transparent decision matrix for calculating administrative fines;**

- **foster "self-regulation" amongst SAs themselves through the commitments in a Memorandum of Understanding (MoU), to complement the GDPR cooperation processes.**

- **consider working in the longer term on the basis of a panel of three CSAs, set up to coordinate a single composite response to a proposed LSA decision; and**

- **provide for a presumption that the LSA approach will be accepted unless there are compelling reasons against doing so.**

24 September 2021

GDPR Enforcement Cooperation and the One-Stop-Shop
Learning from the First Three Years

The GDPR has been in force for more than three years. One of the defining elements of the GDPR is its innovative approach to Supervisory Authorities (SA) cross-border enforcement, generally referred to as the One Stop Shop (OSS). CIPL[5] publishes this white paper (Paper) to identify possible solutions to improve the OSS mechanism.

Background

The OSS provides that the SA of the main or single establishment of the controller or processor (the Organisation) is competent to act as lead SA (LSA) for that Organisation's cross-border processing[6] in accordance with the cooperation procedure.[7] The LSA acts as sole interlocutor for the Organisation with respect to enforcement decisions relating to the cross-border processing.

The LSA is, therefore, in the position to develop a body of knowledge about and expertise in the operations of the relevant Organisations as well as increased efficiency in enforcement. The LSA can utilize such in-depth understanding to determine the appropriate regulatory responses to Organisations with a view to ensuring compliance for the benefits of individuals. The OSS is subject to a complex arrangement under which SAs from other jurisdictions (Concerned SAs or CSAs) may have views in enforcement actions. This occurs where the LSA makes an enforcement decision with respect to cross border processing which impacts individuals in the jurisdiction of the CSA. The LSA and the CSAs have the obligation to cooperate with one another with the objective of reaching a consensus.[8] In the event that the SAs are unable to agree between themselves, the matter is referred to the European Data Protection Board (EDPB) for final decision.[9]

The OSS is a ground-breaking attempt to introduce a form of 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 OSS proved to be highly debated during the passage of the GDPR but also one of the essential elements supporting the public policy goal of uniform enforcement and fruition of data protection rights across the EU,** which could not be achieved under the fragmented enforcement model of the old Data Protection Directive, where each SA was competent to enforce data protection rules in their own territory. At the same time, the OSS had to remain consistent

[5] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 80 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. 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.

[6] See definition of "cross-border processing" in Article 4(23).

[7] See Article 56(1) and Article 60.

[8] See Article 60(1).

[9] See Article 65.

with the EU Treaty providing for independent authorities to oversee compliance with data protection rules,[10] as well as the fundamental right to an effective remedy before a national authority.[11]

The OSS is beneficial to Organisations as their processing activities are increasingly performed across territories to serve clients/users in multiple countries or to support multi-country corporate operations. Consequently, the OSS is likely to come into play quite often, thus ensuring that Organisations are not subject to enforcement for identical processing operations in different member states. This generates lower compliance costs for organizations, as well as legal certainty for all stakeholders on the realisation of data protection rights. In addition, Organisations and individuals can reasonably expect fair, proportionate, transparent and consistent regulatory decisions across the EU.

Despite the fact that the OSS has been part of the law since the GDPR came into effect, it has repeatedly been subject to vocal criticism from some quarters. While some of the criticism from privacy activists might be expected, it has also been attacked by a number of SAs.[12] We note that this institutional criticism may be partly fueled by fear that the OSS **would imply a "loss of independence or powers" for CSAs in contrast to the old, fragmented model.[13] Nevertheless, this hesitation finds no place in the GDPR, which intentionally provided for the OSS as a cornerstone of a harmonised data protection regime.**

The June 15, 2021, decision of the CJEU in the case *Facebook v. Gegevensbeschermingsautoriteit*,[14] confirmed that the OSS is essential for the proper and effective operation of the GDPR. Since Article 56 of the GDPR provides for competence of the CSA in specific cases (including the ability to seek judicial enforcement against the organisation), this is to be considered a limited exception to the general rule that the LSA is competent for the enforcement of cross-border processing.

It is clear that there is considerable investigatory and enforcement activity in the EU. Out of the 1,482 cases listed in the IMI register[15] maintained by the EDPB, 539 cases come under the OSS and 110 cases are subject to final decisions.[16] However, these figures cannot hide the concerns raised about the workings of the OSS. These appear to be attributable to a number of main factors:

[10] See Article 16 of the Treaty on the Functioning of the European Union (TFUE).
[11] See Article 13 of the European Convention on Human Rights.
[12] See Politico article, dated December 27, 2019, reporting on complaints by the SA from Hamburg of "delays" in enforcement by the Irish SA. See also Politico article, dated December 2, 2020, reporting on the Hamburg SA considering challenge to Irish SA Twitter penalty.
[13] See Balboni, Pelino, & Scudiero (2014), Rethinking the one-stop-shop mechanism: Legal certainty and legitimate expectation, Computer Law & Security Review, Vol. 30(4), p. 396: 'We understand that, behind the resistances to embrace a full OSS system, there may be the fear that some DPAs will somehow take the "lion's share" of the whole proceedings involving major controllers and/or the fear that such model implies a loss of independence or powers for the (other) DPAs. As to the first point, this is basically a political issue rather than a legal one, and, as such, should be addressed openly and frankly.
[14] Case C-645/19. See also conclusions of the Advodate General Bobek, point 47 and seq.
[15] The EDPB created a dedicated workflow in the Internal Market Information (IMI) register to enable SAs to cooperate and to facilitate the SAs in identifying their respective roles of LSA and CSA.
[16] EDPB OSS register https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en.

- the **division between the regulatory powers** of national SAs and the involvement of CSAs in final decisions;

- the **lack of EU harmonised administrative procedures** and judicial appeals to handle OSS cases (such as, for instance, position of the parties in the proceedings, including complainants, admissibility criteria, duration of proceedings, deadlines, possibility to share confidential information with other SAs and with the entity undergoing the investigation, grounds of judicial appeals in the LSA's courts), different interpretations of concepts relating to the cooperation mechanism and different approaches regarding, for instance, the start of the cooperation procedure, the timing of involvement of CSAs, and the communication of relevant information to them. This lack of consistency in administrative procedures and lack of efficiency in handling cross-border cases has been highlighted both by the EDPB[17] and the EU Commission;[18]

- the **cultural and strategic differences between SAs**, also rooted in the different legal traditions found across the EU, which may mean different approaches on how to best enforce the GDPR: some who regard enforcement and punishment as their primary role and whose activity is mostly "complaint driven;" others who take a broader view of the regulatory options, see their role as being more strategic. They may, for example, focus on achieving compliance by engagement and see enforcement as a last resort. This results in diverging views between SAs as to the type of cases which should be prioritized or not depending on their trivial or serious impact on the rights and freedoms of individuals;

- the diverging approaches on the **role and prerogatives of the LSA**. Some SAs viewing this as a "primus inter pares role," limited to bringing all DPAs views together and finding a common denominator between the different approaches of the CSAs, while others see the role of the LSA as an independent regulator driving the enforcement procedure and making strategic choices, subject to the cooperation procedure. The intrinsic complexity of conciliating the independence of the regulator with the GDPR mandate for consistency has been highlighted by the EDPB in its recent binding decision ordering the LSA to perform a statutory investigation on data uses in the WhatsApp/Facebook case.[19] The degree of discretion of the LSA needs, therefore, to be better defined, understood and accepted;

---

[17] See Contribution of the EDPB to the evaluation of the GDPR under Article 97, adopted on 18 February 2020, page 10. See Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities, page 23.

[18] See 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 COM(2020) 264.

[19] "Whilst the EDPB considers that SAs enjoy a certain degree of discretion to decide how to frame the scope of their inquiries, the EDPB recalls that one of the main objectives of the GDPR is to ensure consistency throughout the EU, and the cooperation between the LSA and CSAs is one of the means to achieve this. Therefore, the EDPB calls upon the LSA to make full use of the cooperation tools provided for by the GDPR (including Articles 61 and 62 GDPR) while carrying out such investigation." See Urgent Binding Decision 01/2021 on the request under Article 66(2) GDPR from the Hamburg (German) Supervisory Authority for ordering the adoption of final measures regarding Facebook Ireland Limited—12 July 2021

- a **frustration in some SAs at the role of the LSA** as sole interlocutor which may be perceived as undermining the role and autonomy of CSAs and lead to efforts to sideline or avoid the OSS, for example by using alternative procedures or by relying on legal mechanisms outside the scope of the GDPR for enforcement purposes;

- the **lack of experience of the LSA** in handling the complexities of cross-border issues, including technical issues, interaction with disciplines not harmonised at EU level (labour, financial, health or contractual laws), interpretation of balance with other fundamental rights and freedoms;

- the opportunity to refer **preliminary questions on the functioning of the OSS** lies with the discretion of national courts and is subject to national laws;

- the **agenda and priorities** of SAs being increasingly set by privacy activists leveraging the OSS and all legal avenues[20] to bring cases forward (including general ideological complaints against a particular business model), thus preventing SAs with limited resources to execute their strategic priorities;

- the **influence of national politics** on the application of OSS and conflicting perspectives shared by Member States with respect to the regulation of technology companies, which has a spillover effect on the activities of SAs to promote sanctioning; and

- the **perverse incentive of huge fines** being possible under the GDPR. These are imposed by SAs on a national basis and make their way into national coffers, as opposed to being part of a common pot for GDPR compliance work throughout the EU. This creates a conflict of interest among SAs that ultimately undermine the effective application of the OSS and the public policy goals of the GDPR. Also, with the e-privacy and GDPR overlap, there is the risk in certain jurisdictions that the level of GDPR fines would be used at a national level for sanctioning e-privacy infringements, at the risk of multiplying "GDPR-level" fines by 27.

In this paper, CIPL considers:

1. **how the OSS, as currently implemented, may be faring in delivering an integrated pan-EU enforcement mechanism for cross border processing activities;**
2. **whether the processes and procedures adopted are providing sufficient fairness, consistency and transparency for all those impacted by the OSS;**
3. **how the OSS should be considered with the enforcement of other digital initiatives, such as e-Privacy;**
4. **whether, overall, the OSS may be delivering and/or supporting effective regulation for organisations and individuals;**
5. **how the OSS is interfacing with the role and functions of individual SAs; and**
6. **What could be proposed improvements to the working of the OSS.**

[20] According to Article 78(2) if the GDPR, individuals have the right to an effective judicial remedy where the competent SA does not handle a complaint or does not inform the individual within three months on the progress or outcome of a complaint.

1. **The OSS may be faring in delivering an integrated pan-EU enforcement mechanism**

Before the GDPR came into force, European data protection laws were enforced by each SA separately for each individual country in the EU. As a result, companies operating across internal EU borders often faced the need to interface with multiple regulators on the same set of facts–in the worst case, dozens or more regulators could be involved. This was unmanageable for companies and effectively dis-incentivized them from trading across different EU Member States within the internal market. It was also an inefficient waste of resources for regulators, given that the questions asked and issues handled underlying each matter were the same.

The development of an integrated pan-EU enforcement mechanism for data protection was, therefore, an achievement of the GDPR. The OSS is also key to the successful implementation of the GDPR. It represents a significant step toward improved European integration and simplifies the functioning of the single market. Under the GDPR, the legal regime is harmonized between Member States.

The powers of the independent SAs are set out in Articles 51 GDPR onwards. While these are the same for all SAs, they are implemented in each Member State under national law. For many of the SAs, their powers predate the GDPR and such SAs have developed their own experience and culture before the GDPR was adopted. Each SA will also set its own regulatory policy and apply national procedural rules of investigation and process, taking into account how their decisions might be appealed before local courts. More generally, SAs must operate within their local systems of public and administrative law. Finally, effective data protection must take into account other legal disciplines that are not necessarily harmonised at the EU level (e.g., labour, health or contract laws). Therefore, while the GDPR is a harmonization measure, the practice of regulation leading to enforcement is guided by pre-existing structures which are not harmonized and need to be reassessed to account for the OSS.

The OSS is still in its infancy and SAs and the EDPB need more time and experience to make the OSS fully operational. In parallel, it has also become clear that, in order for the enforcement decisions of LSAs to be accorded proper weight and respect, SAs must also give mutual recognition to the regulatory processes and decision-making capacity of other Member States. SAs should seek to understand and should acknowledge and show appropriate administrative deference for the regulatory policies, approaches, views and actions of other SAs, observing explicit principles of mutual respect and self-restraint, with the default position of not challenging the judgment and proposals of another SA, taking into account the constraints that may exist under national procedures and the different legal traditions of Member States. **The EDPB has been working toward enhanced transparency and awareness on the different legal systems and administrative practices, with a view to enhance the common working of SAs.[21] CIPL supports this approach and recommends that regulatory policies and practices be further systematically shared, explained and mutually understood between SAs as this will lead to an enhanced level of harmonization at a high level, drawing on best practice among SAs.**

So far, it appears that there have been shortcomings in this element of understanding and respect for equivalence. A specific example can be seen in the case taken by the Irish SA regarding Twitter under Article 65(1)(a) GDPR concerning a personal data breach. No fewer than eight CSAs raised objections to

[21] See Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities.

the decision,[22] some of them questioning the fine calculation even though the GDPR awards SAs discretionary power for penalty setting and no single methodology exists on how to calculate GDPR administrative fines.[23]

As such, the OSS appears to be reflecting the stresses and tensions which have been experienced in other areas (such as food safety, pharmaceuticals, product safety and competition) where mutual recognition of other States' law and procedures has been required in order to successfully adopt a consistent approach throughout the EU.

Fine calculation appears to be a torn issue with SAs adopting their own perspectives of what constitutes a deterring fine and which fines are "too low." It is beyond the scope of this Paper to carry out a detailed assessment of this area, **but we note that such tensions have occurred in other areas and would draw attention to techniques which have been employed to address the problems. Similar to the GDPR, European antitrust law allows for fines as a percentage relative to a company's total worldwide annual revenue. However, there are specific guidelines issued by the European Commission and which outline the precise methodology to be used when determining the final penalty in antitrust cases**. While this methodology takes into account factors which are specific for the antitrust environment, they may serve as a reference point for SAs and minimize frictions by serving as an objective benchmark with which to calculate fines, where these are deemed the best enforcement mechanism for ensuring GDPR compliance taking into account the circumstances of the infringement.

Settlements are also an area of possible improvement in consistent approaches to foster more effective GDPR implementation and enforcement. The EU Parliament[24] regretted that some SAs enter into settlement to close cases instead of issuing a sanction. CIPL underlines that settlements providing for commitments can actually foster better compliance as internal oversight systems and processes serve to ensure that such commitments are delivered. This is demonstrated in other regulated areas (competition law, anti-corruption). Learnings can also be obtained from the EU Consumer Protection Cooperation Network regarding achievements obtained from the acceptance of traders' commitments. It is also embedded in the draft EU Commission Digital Service Act.[25] CIPL would welcome EDPB guidance on how settlements can be used as an alternative to requiring every case to complete the full Article 60/65 GDPR process in those Member States which permit such settlement. Given the specific mechanism of the OSS, this may also require setting specific rules to make the transactional agreement available to the CSAs as well. This has the potential to enable resource savings at both the national and EDPB level, the potential

[22] See Binding decision of the EDPB under Article 65 GDPR Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(10(a) GDPR Adopted November 2020.

[23] See the WP29 Guidelines on the application and setting of administrative fines (wp253), endorsed by the EDPB. See also Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679. See CIPL's response to the EDPB consultation.

[24] European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application.

[25] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final Article 41(2)(a) "Where needed for carrying out their tasks, Digital Services Coordinators shall have at least the following enforcement powers, in respect of providers of intermediary services under the jurisdiction of their Member State: (a) the power to accept the commitments offered by those providers in relation to their compliance with this Regulation and to make those commitments binding."

for much faster outcomes, and faster compliance. For example, where there is a cross-border processing registered in the IMI system, the EDPB may provide guidelines on when that process could be resolved via commitments and an agreed settlement, or when a LSA can propose a settlement with commitments for approval in place of a draft decision.

Another example is the Report by the European Parliament on the implementation of the European Arrest Warrant (EAW) and the surrender procedures between Member States[26] which noted that **the principle of mutual recognition must be premised on mutual trust. The development of such trust and improved workings in that field has been and continues to be developed by a number of approaches which could usefully be adopted by the EDPB.** These include:

- shared training of decision-makers and experts involved in the field;
- exchanges of information and learning;
- soft-law assistance such as manuals on procedures to be adopted;
- guidance in the EAW area on specific definitions such as the term "judicial authority" prepared by Eurojust; and
- work to increase common understanding of best practices in regulation.

CIPL believes that similar techniques could be used by the EDPB, encouraged by the Commission, to improve the working of the OSS.

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.

The EDPB has started to move somewhat along these lines. In its document "EDPB Strategy 2021-2022,"[27] under the heading, "Supporting Effective Enforcement and Efficient Cooperation Between Supervisory Authorities," it states that it will aim, not only to promote efficiency in the cooperation and consistency mechanism but, *"[. . .] to strive for the development of a genuine EU-wide enforcement culture among supervisory authorities. Therefore, it will actively endeavour to fulfil its role as a forum for the regular exchange of information on ongoing cases."* CIPL notes, however, that such a culture must not only seek to be consistent, but also be fair, proportionate, accountable for the economic and social impact of data protection decisions, and learn from best practices and past issues experienced among regulatory bodies in Member States concerning the implementation of the OSS mechanism.

[26] The Implementation of the European Arrest Warrant and the Surrender Procedures between Member States 2019/2207(INI).

[27] EDPB Work Programme 2021/2022, adopted on 16 March 2021.

The EDPB has also taken steps to establish a pool of experts to exchange expertise among authorities to help in cases.[28] The experts may be external experts or EDPB members who can offer experience relevant to an investigation or enforcement activity. In both these initiatives, the focus is on the specific tasks of investigation and enforcement.

The EDPB further plans to develop guidance on the following areas:

- guidance on Art. 60 GDPR–One-stop-shop
- guidance on Art. 61 GDPR–Mutual assistance
- guidelines on Article 65 GDPR
- guidelines on the calculation of administrative fines
- assessment of the practical implementation of the amicable settlement

These initiatives are welcomed by CIPL. However, CIPL would support the development of a broader base of common understanding of problems, procedures and regulatory techniques, as well as specific enforcement models utilizing techniques such as those used in work on the EAW.

2. Processes and procedures followed—fairness consistency and transparency

Few things are more detrimental to effective regulation than a lack of trust and respect not only among the SAs but also from the regulatees. This can erode willingness to engage with SAs, a willingness which is critical in the world of developing technologies. One of the specific concerns about the working of the enforcement process and the OSS among CIPL members has been the different approaches taken by SAs in enforcement actions. For example, some SAs give detailed preliminary notice of intent to consider action, others do not accept representations before decisions are made, or timescales for representations differ. Whilst SAs are, of course, entitled to progress inquiries as they see fit and in accordance with the provisions of the GDPR and the concept of fair procedures, we would encourage SAs to adopt a harmonised approach to inquiries where permitted by the circumstances of the cases presented before them. These fair procedures should include clear timelines and opportunities for full answer and defense.

This feedback reflects the challenges identified by the EDPB itself in its 2020 report.[29] The EDPB identified as main challenges, the differences in national administrative procedures, concerning, in particular: complaint-handling procedures, position of the parties in the proceedings, admissibility criteria, duration of proceedings, deadlines, the possibility to share confidential information with other SAs, concrete consultation of the CSAs on draft measures and different interpretations by SAs of concepts relating to the cooperation mechanism such as "relevant information" "without delay" and "draft decision."[30]

CIPL welcomes the work program adopted by the EDPB, described above, which seeks to address some of these difficulties. It recognises that many of these challenges cannot be finally and conclusively solved by the EDPB and SAs alone. In the long term, it may suggest the need for legislative action in a form similar

[28] https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-terms-reference-edpb-support-pool-experts_en, adopted December 2020.
[29] See Contribution of the EDPB to the evaluation of the GDPR under Article 97.
[30] Other factor such as different approaches of national courts and appeal mechanisms can also play a major influence in the lack of consistency.

to the ECN 2 Directive in antitrust, creating a common set of basic procedural rules across the EU.[31] However, CIPL believes that, in the short and medium term, the recommendations in this paper could be adopted and bring considerable improvement to the current position.

In the GDPR, there are only limited transparency obligations with respect to enforcement. However, this is an area where transparency is critical to engender trust. CIPL recognises that Member States have separate administrative and procedural rules which may have an impact in some cases. To the extent it is possible within Member State laws, **CIPL would strongly support the development of a common framework for procedural rules for the stages of supervisory action by SAs under Chapter VII of the GDPR. CIPL welcomes the EDPB guidance on transparency and procedure which has been put forward in the draft Guidelines 03/2021 on the application of Article 65(1)(a) GDPR. It supports the development of such rules including:**

- clearly setting out the restricted circumstances in which exceptions to the power of the LSA may apply (over urgency matters, or when matters affect only individuals in one Member State);
- ensuring that regulatees have access to all the evidence to be considered in a case;
- providing the right to make representations to SAs before formal action is taken;
- the adoption of common timescales for Chapter VII procedures;
- increasing transparency to regulatees, for example, by making them aware of any relevant and reasoned objections made to a proposed decision, and to make representations to the EDPB where appropriate, including the right to be heard in enforcement cases where fines or other sanctions could be imposed;
- rigorous transparency in the OSS process on all elements of the file vis-à-vis the CSA, including a requirement that a LSA should include in any draft decision, clear explanations of any decisions on the scope and nature of its investigation, in particular where the complainant asked for wider investigations and/or the circumstances might clearly indicate that wider investigations might have been pursued; and
- enhanced transparency for individuals by publishing relevant interactions between SAs on the EDPB website to foster greater accountability amongst SAs.

Lastly, CIPL encourages the adoption of increased transparency, not only on the enforcement side, but also in the EDPB's regulatory subgroups and task forces composition and activities, as well as more consistent regulatory approaches.

[31] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0001.

3. How the OSS should be considered with the enforcement of other digital initiatives?

In its opinion in *Facebook v Gegevensbeschermingsautoriteit*, the Advocate General Bobek clarifies that: (1) the e-Privacy Directive and the GDPR may apply at the same time, or may not, depending on the actual provision that has been allegedly breached and (2) that the OSS does not apply to the e-Privacy Directive.[32]

This potential overlap of enforcement regimes is a sensitive area in which the possibility of double jeopardy–an unacceptable outcome incompatible with basic legal rights and the rule of law as set forth in both the GDPR and the EU Charter–remains a threat to organisations. The interface between the GDPR and the e-Privacy Directive is very close though the requirements of those laws are, at times, inconsistent with one another. For example, in some cases, the GDPR may permit the processing of personal data in accordance with legitimate interests, whereas e-Privacy may require the collection of consent from the individual for the exact same process. There are cases which could potentially be treated as falling into either regime but result in different outcomes depending on whether the GDPR of the e-Privacy Directive is applied. In *Facebook v. Gegevensbeschermingsautoriteit*,[33] the Belgian SA alleges unlawful collection and use of information by means of cookies on the basis of the national Belgian law implementing Directive 95/46. The French SA takes a different approach in the case against Google and Amazon by sanctioning the lack of transparency and consent on the placing of cookies on the basis of French law implementing the e-Privacy Directive.

In cases where the GDPR and the e-Privacy Directive apply to the same processing activity, the organisation may be dealing with a LSA concerning the GDPR aspects of a matter, but a national SA may take parallel actions regarding the e-Privacy aspects, although the factual issues are the same or relate to the same processing.[34] In such case, SAs go as far as applying GDPR rules to assessment of applicable law and administrative sanctions when enforcing the e-Privacy Directive but dismiss the application of the OSS. The EDPB should clarify that the e-Privacy enforcement regime cannot be used as a backdoor to enforce GDPR rules and the range of sanctions under GDPR while bypassing the GDPR OSS mechanism. SAs must work together to avoid these outcomes by forgoing enforcement on identical facts under these separate legal regimes.

The situation may get even more complex if the upcoming e-Privacy Regulation fails to align the two enforcement regimes by applying the OSS mechanism as set forth by the GDPR. Now that the e-Privacy Directive is a Regulation that is directly applicable in all Member States, it is necessary that the OSS ensure the harmonisation objectives of the regulation are met at all stages, including at the enforcement level, to avoid recreating the fragmentation that the regulation is seeking to address. This would also make sense as the e-Privacy Regulation is considered as a *lex specialis* to the GDPR that it is supposed to

[32] See Case C-645/19. See also conclusions of the Advodate General Bobek, paragraph 36 and seq.
[33] In this case, the Belgian SA is not acting as LSA as the proceedings where initiated before the GDPR became effective. See Case C-645/19.
[34] See, for instance, the case launched by France Digitale against Apple, which is handled by the CNIL under the e-Privacy Directive. This follows a similar case handled by the Irish DPC on the basis of the GDPR. https://www.hebergementwebs.com/apple/apple-vs-france-digitale-the-cnil-takes-up-the-case.

particularise.[35] This position is also fully supported by the EDPB.[36] Unfortunately, at this stage the common position of the EU Council for the future e-Privacy Regulation does not include the OSS mechanism for cross-border cases enforcement. It only provides that "[e]ach supervisory authority shall contribute to the consistent application of this Regulation throughout the Union and cooperate with each other and with the Commission."[37]

The absence of OSS in the e-privacy landscape would go against the principle of the free movement of services by creating clear inefficiencies that might also have the effect of excluding smaller operators from creating EU-wide services. In addition, this would give rise to the possibility of double jeopardy with resulting decisions requiring outcomes which may conflict depending on the legislative regime applied. This situation should be addressed by the EU institutions in developing the enforcement and supervisory regime under the revised e-Privacy Regulation.

Finally, it is critical that the GDPR OSS efficacy be improved so that it serves as a blue print for other upcoming digital initiatives where organisations would benefit in having a single point of contact or interlocutor on enforcement matters, such as the draft AI act, the draft Digital Services Act, or the draft Data Governance Act.

4. Is the OSS delivering and/or supporting effectiveness for Organisations and individuals?

This question raises the gap between the role of the LSA, the role of the EDPB and the functioning of the OSS. It, of course, also begs the question of what amounts to effective regulation. There are significant rifts—in theory and practice—between different approaches to the effects, if any, of financial and other corrective measures. These demonstrate fundamental tensions over the consistency and coherence of EU enforcement policy. The basic conflict is between the traditional "economic" concept of deterrence through sanctions and outcome-focused compliance, which focuses on changing behaviour in practice with respect to the (also) fundamental freedom of establishing a business and being accountable for the economic and social impact.[38]

CIPL has carried out a range of work on the issue of effective regulation.[39] CIPL's view is that, at its core, effective regulation needs to recognise that:

- SAs should adopt transparent strategies, spelling out desired outcomes, their approach, and their priorities;

[35] See https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/.
[36] See EDPB Statement 03/2021 on the e-Privacy Regulation of 9 March 2021, *"Oversight of privacy provisions under the ePrivacy Regulation should be entrusted to the competent supervisory authorities under the GDPR to further support consistency."*
[37] Draft regulation concerning respect for private life and the protection of personal data in electronic communications and repealing directive 2002/58/EC (regulation on privacy and electronic communications) – Council mandate. See draft Article 20 on Cross-border cooperation.
[38] Comments on GDPR Enforcement EDPB Decision 01/020 by Prof. Christopher Hodges (March 2021).
[39] See Regulating for Results: Strategies and Priorities for Leadership and Engagement (October 2017).

- All those involved (SAs, individuals and regulatees) need to have a realistic agreed view of what constitutes appropriate levels of compliance, with shared understanding of standards which should be met;

- Regulatees should commit to work to or toward those standards, but have clear expectations of the possible/likely outcomes if they fail to do so;

- SAs must be honest, transparent, fair and independent in enforcing standards where appropriate;

- SAs must be accountable of the balance among fundamental rights and freedoms at stake as well as of the economic and social impact of their decisions;

- "Deterrence" through enforcement and punishment is less effective in practice than "constructive engagement" which educates and builds on the "enlightened self-interest" of regulatees; and

- Those who deliberately, cavalierly or repeatedly flout the requirements have no hiding place.

In such an environment, regulators and organisations share mutual respect and operate in an atmosphere of genuine dialogue, where regulatory enforcement is tied to evidence-based rationales that promote higher level of data protection.

In addition, a range of tools can help SAs and organisations achieve compliance based on a common understanding of required standards, such as setting up regulatory sandboxes to explore the application of the law to new areas,[40] promoting the development of codes of practice covering specific types of processing or applying mitigating factors taking into account the circumstances of the case and the compliance efforts of the organisation in enforcement cases. SAs can also set deadlines for meeting standards, draw "lines in the sand" with timelines to make clear when they will take action. These are all tools in the area of transparent and fair regulation. It also enables SAs to better allocate their limited resources toward driving compliance on the market to the benefits of individuals in line with their strategic goals.

Effective regulation is undermined in cases where these criteria are not met, for example where action is taken without any warning especially in cases where there is real uncertainty about the scope of the law, or where rules that allocate competence are not respected. This results in legal uncertainty and increased compliance costs for SAs and regulatees.

This is particularly apparent where SAs take different views relating to competence or enforcement and continue to dispute the application of OSS in complaints they receive, where these should be routed to the LSA. In such cases, organisations who have a bona fide interest in continuing to engage with the LSA and achieving compliant outcomes which satisfy the requirements of the GDPR may be subject to repetitive and costly administrative procedures as a result of the OSS being challenged. This is in addition to a significant risk of double jeopardy (see previous section) or situations where sanctions are applied in cases where the organisation believed it had realistically met the required standards, where penalties are

[40] Regulatory Sandboxes in Data Protection - Constructive Engagement and Innovative Regulation in Practice, March 8, 2019.

seen as being out of proportion to the non-compliance, where reasonable efforts are not taken into account, or where organisations are not given open and fair hearings before decisions are made.

While CIPL understands that SAs may have the obligation to address the complaints they receive subject to potential judicial remedy against an SA,[41] there should be a better collective thinking as to what constitutes a complaint likely to impact the rights and freedoms of individuals. In other words, SAs should collectively agree to differentiate between "fundamental complaints" impacting the rights and freedoms of individuals, as opposed to pure technical breaches of the GDPR that only relate to formalistic compliance, and can be addressed through other means than the complaint based model. In this respect, the EDPB should encourage the setting of prioritization criteria to ensure that SAs' intervention are prioritized on issues having a significant impact on fundamental rights.[42]

The EDPB is not itself a regulator *stricto sensu*, as has been noted already, there is accordingly a gap between the development of effective regulation under the GDPR and the work of the OSS. In the formal work of the OSS, the EDPB can only step in at the final point of decision. In a sense this is a structural problem created by the GDPR. Furthermore, while the EDPB has been active in developing guidance to assist SAs and support the application of the OSS, there is a gap between the development of guidance and its application in practice. In practice, industry may need to take steps to interpret and operationalise newly articulated requirements. In this context, there should be more communication between SAs and organisations to raise awareness on the one hand on the SA's expectations and on the other of market practices with the ultimate goal to encourage and foster compliance.

It is noted that the EDPB has started work on the coordination of regulatory activity. It has published a Document on a Coordinated Enforcement Framework adopted 20 October 2020.[43] However, this is only of limited scope. It proposes to select one topic for an annual review by SAs who elect to join the process. While this initiative is welcome, **CIPL would advocate more in-depth training and engagement with SAs in a more systematic manner and which is also conscious of the administrative autonomy of SAs. This could be done by addressing cooperation models for regulatory behavior and approaches, possibly under the banner of the Article 60 GDPR procedures and would be aimed at developing effective and consistent regulatory strategies which focus on desired outcomes (such as improvement of compliance practices) rather than "enforcement" for its own sake.**

5. How is the OSS interfacing with the role of individual SAs handling local cases?

The aim of having SA locally handle cases is primarily intended to resolve matters for the complainant(s) that are not linked to cross-border processing activities and to ensure outcomes which comply with the requirements of the GDPR as articulated by the local SA.[44] That was the basis of the decision to ensure

[41] See Article 78(2).
[42] See, for instance, DPC Regulatory Strategy APRIL 2021 Public Consultation.
[43] See https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/edpb-document-coordinated-enforcement-framework-under-regulation_en /. See also the EDPB taskforce set up in September 2020 to process and uniformly respond to complaints received by SAs following the Schrems II CJUE judgment. In its statement on the creation of the taskforce, the EDPB indicated that the taskforce will ensure a close cooperation among the members of the EDPB.
[44] In addition to cases specifically entrusted to the local SA under Article 55(2) of the GDPR (processing carried out by public authorities, processing carried out in the public interest or in the exercise of official authority).

that individual SAs could deal with local cases. These cases should be distinguished from the provisions of Article 56 (2) GDPR that enable a local SA to handle cases involving cross-border activities by exception to the OSS mechanism in limited cases (the subject-matter of the complaint relates only to an establishment in the local state or affects individuals in that state only) and in accordance with the GDPR cooperation mechanism.

In any case, there should be a sharp distinction between the resolution of a one-time isolated infringement case by the local SA and the handling of systemic non-compliance with law by a LSA which affects individuals in multiple countries. This distinction should impact the investigation and handling of the cases, the nature of the relevant enforcement decisions and corrective measures, the level of any fines and the calculation of the relevant caps which should be differentiated at the LSA and SA levels.

LSA cases:

It is of the utmost importance that the LSA is able to independently investigate and handle cross-border cases. The independence of the LSA coupled with its cooperation obligations under the GDPR enforcement provisions also require full transparency on the investigation and sharing the file with CSAs. This also includes taking into account CSAs views and interpretation of the law and the particular case. But this should not de facto mean that the LSA should be bound by any CSA prior assessment of whether and how individual rights have been or risk being impacted. Because the LSA acts as the primary interlocutor with the organisation and has some experience handling cases and interacting with this organisation, it may have a different view than CSA that is by definition more locally driven. As a consequence, 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. As a matter of fact, 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 and 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." Similarly, AG Bobek explains that,

> [w]here the alleged infringements concern cross-border processing and an authority is not the LSA, other supervisory authorities should be able to examine the matter in order to provide a meaningful input when called upon to do so within the framework of the cooperation and consistency mechanisms, or to adopt urgent measures. However, it is then for the LSA to, generally, adopt binding decisions to enforce the GDPR vis-à-vis the processor or controller.

AG Bobek also rightly explains that multiple SA action does not result in more and better protection of individuals, confirming that the OSS and the prominent role of the LSA enables a high level of protection of the rights and freedoms of individuals because it is more coherent, effective and transparent.

In addition, in LSA cases, CSA should also ensure 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.[45] This means that, to the extent permitted by law, the CSA should push back on unrealistic and frivolous requests or complaints from entities trying to test the OSS system where there is no real risk to the rights and freedoms of individuals at stake. In other words, the CSA should not just automatically pass on any request or complaint to the LSA without first assessing whether it can constructively impact the handling of the investigation and, as the case may be, endeavor to resolve this locally. As such, prior engagement between SAs and organisations on individual complaint cases, to give the organisation the opportunity to resolve the complaint, would act as an initial triage process and would avoid too many unresolved cases being brought to the LSA.

Local SA cases

In order to meet the tests of proportionality, punitive sanction by a national SA for a national law breach must be proportionate to the impact in that jurisdiction. The determination of the maximum amount of the fine and the calculation of the fine cannot simply be related to overall global turnover where individuals are affected at national level only. The imposition of high levels of fines calculated on the basis of the overall global turnover for local cases which do not involve individuals from multiple jurisdictions runs a real risk of double jeopardy (as the level of fine is calculated as if there were individuals from multiple jurisdictions involved and the organisation may be sanctioned several times for the same processing activity). This situation is made worse by the fact that other EU regulatory regimes which regulate data directly or indirectly do not rely on the OSS. Different regulators may develop different thresholds for initiating investigations, which may overlap with on-going investigation into the same matter, with different drivers and objectives, with different procedures, language, intake forms and dynamics. Challenges may be significant and the level of resources to address them may be prohibitive for new potential entrants into the market.

6. Proposed improvements to the working of the OSS

To support the OSS, and to implement the recommendations set out in this Paper, the EDPB and SAs will need to demonstrate commitment to concrete action. In addition to the recommendations already made throughout this Paper, CIPL believes the following proposed actions may improve the functioning of the OSS. The powers of the EDPB, as set forth in (i) Article 70(1)(a), to monitor and ensure the correct application of GDPR in the cases provided for in Articles 64 and 65 without prejudice to the tasks of SAs and (ii) Article 70(1)(u), to promote the cooperation and effective bilateral and multilateral exchange of information and best practices between SAs, could enable the **EDPB to lead on the development of a register for validating single or main establishment for which a specific LSA should be competent under**

[45] See AG Bobek opinion on describing the leading role of the LSA in the OSS mechanism "the EU legislature has decided to emphasise the centrality of the LSA's competence even before detailing the specific tasks and powers of *all* supervisory authorities." See recitals 59 and 60 "share the view of the Board which, in a recent Opinion, referred to Article 56(1) of the GDPR as an 'overriding rule' and as '*lex specialis*': that provision 'takes priority [over the general rule of Article 55 of the GDPR] whenever any processing situation arises that fulfils the conditions specified therein [. . .] I believe that the DPA and certain governments misinterpret Article 55 and Article 56(1) of the GDPR." Those interveners take the first part of the sentence in Article 56(1) out of its context, in order to reverse the relationship between the rule and the exception. To do so results in watering down the prescriptive content of several provisions of the GDPR, and frustrates the objective, emphasised inter alia in recital 10 thereof, of ensuring a more consistent and homogenous application of the data protection rules. It would essentially amount to a return to the previous regime of Directive 95/46.

the OSS and a Protocol, Code or Memorandum of Understanding (MoU) between SAs which further supports the application of the OSS mechanism.

1. Organizations should be allowed to submit an application to their selected SA for validating their single or main establishment that triggers the application of the OSS under the GDPR, thereby ascertaining the LSA which is competent to monitor compliance with respect to their cross-border processing activities. This could be validated/accepted by other SAs under the cooperation procedure and placed on a register run by the EDPB on a voluntary basis. This register could be made available on the website of the EDPB and serve as a reference point for SAs and individuals. In the event of conflict which cannot be resolved, the issue may be decided by the EDPB under Article 65(1)(b), but voluntary cooperation procedures before conflicts arise would improve efficiency of GDPR enforcement and reduce administrative costs for SAs and compliance costs for organizations having to repeatedly assess whether the OSS applies. This would not contradict the WP 29 Guidelines for identifying a controller or processor's lead supervisory authority adopted in April 2017.[46] Having a formal procedure for signing off on the application of the OSS with respect to the organisation's activities would promote the success of the OSS, while serving as a transparency mechanism that promotes further accountability and legal certainty, taking into account the complex reality of business organisations.[47]

2. An MoU (or protocol or Code) could address several of the problems identified in this Paper. CIPL believes that the concrete steps recommended above do not need to be imposed, but can be achieved by "self-regulation" amongst SAs themselves in the form of an MoU. The MoU would be based on Chapter VII of the GDPR and would set out specific commitments accepted by all SAs, whereby all SAs explicitly and transparently commit to observing a set of practical measures in line with agreed principles of mutual respect, administrative autonomy, and self-restraint. It would exist alongside and elaborate upon the more formal procedures of the GDPR, but ensure that those procedures are not invoked inappropriately or prematurely.

    a) For example, there are potentially a large number of CSAs involved in major cases. Adopting an individualistic approach to regulation in such cases leads to duplication of effort by the SAs involved and a backlog of cases as they require intensive negotiations to come to common consensus regarding the appropriate action to be taken. This could be addressed (in the longer term where trust among SAs has increased and the functioning of the OSS has improved) by adopting a "two tier" approach in which a limited number of CSAs would coordinate the response on behalf of others through a mutual recognition procedure (probably most effectively from those countries most impacted). This system used to be particularly efficient for the instruction of BCR under Directive 95/45 where three SAs were handling the file on behalf of other SAs in order to simplify and accelerate the review process. A similar process under the GDPR should be even more efficient and would help increase solidarity between SAs acting as LSAs and those acting as CSAs.

[46] See WP 244 rev.01 at https://ec.europa.eu/newsroom/document.cfm?doc_id=44102.

[47] See CIPL OSS Paper—The One-Stop-Shop and the Lead DPA as Co-operation Mechanisms in the GDPR November 30, 2016, where CIPL highlights the practical challenges faced by organisations to identify their main establishment and LSA (page 6).

b) The MoU could further contain a presumption that the approach proposed by an LSA will be accepted unless there are compelling reasons against doing so. Objections raised by a CSA shall be accompanied by clear evidence of (i) the significance of the risks posed by the draft decision in regard to the due balance to be made of the fundamental rights and freedoms and, if applicable, free flow of data, and (ii) the economic and social impact in the EU of the objection.

c) SAs could also commit in the MoU to develop more expertise in the EDPB around specific issues which may need to be resolved. A special EDPB subcommittee with representation from each SA could be set up. Its sole task would be to oversee and ensure effective management of consistency operations, including but not limited to, disputes arising in relation to OSS. This subcommittee would operate as a common forum and a specialised taskforce governed by common roles with the objective to operationalise and standardise consistency activities. SAs should also commit to devoting specific resources to handle these OSS cases so that they can be trained, gain the relevant knowledge and experience, and enable the system to improve over time. They could also exchange best practices and to further align their views on the interpretation of core concepts relating to the cooperation mechanism in order to improve efficiency. It may also be relevant to promote and prioritise the expert pool of expert exchange programs with SAs' personnel that is involved in handling OSS cases.

More generally, there is much that could be done to improve efficiency and effectiveness to avoid backlogs and other delays, and to ensure strong working relationships amongst all SAs.

By adopting the measures described in this Paper, we believe that consistent decision making by SAs can be encouraged, thereby reducing delays in finalizing decisions in cross border cases, creating a consistent bank of precedent decisions for SAs to leverage, and encouraging organisations to act in accordance with clear, consistent and transparent messaging which represents the views of all SAs.

If you would like to discuss these recommendations or require additional information, contact Bojana Bellamy, bbellamy@HuntonAK.com, or Markus Heyder, mheyder@HuntonAK.com.