November 30, 2016

The One-Stop-Shop and the Lead DPA as Co-operation Mechanisms in the GDPR

CIPL GDPR Interpretation and Implementation Project

November 2016

November 30, 2016

Introduction

The One-Stop-Shop and the Lead DPA as Co-operation Mechanisms in the GDPR

One of the fundamental changes introduced by the GDPR is the mechanism of co-operation between a lead supervisory authority and other concerned supervisory authorities (the "one-stop-shop-mechanism").[1] The lead supervisory authority has a key role within this mechanism. The competence of the lead is triggered by the concept of the main establishment of a controller and/or processor.

The Article 29 Working Party identified the preparation of the one-stop-shop-mechanism—and the consistency mechanism—as priority.[2] This preparation consists of the following building blocks:

- the designation of lead data protection authority;
- the one-stop-shop on enforcement co-operation;
- the EDPB consistency mechanism.

CIPL takes the view that a fully functioning co-operation mechanism among DPAs, based on the concept of a one-stop-shop ("OSS") and a lead DPA, is an essential prerequisite for the consistent and effective implementation of the GDPR. The ambitions of the GDPR are significant, but these ambitions can only be achieved if there is sufficient clarity on the meaning of the relevant GDPR concepts, as well as on their implementation. This also means that the DPAs should act with full transparency when applying these GDPR provisions and should consider the views of the various stakeholders in an appropriate manner.

A fully functioning OSS benefits individuals and the controller and processors with whom they deal. The critical benefit to controllers and processors is the ability to build their GDPR compliance programmes relying on a single or main establishment and a corresponding lead DPA. This gives them more certainty and predictability about their compliance with the new law and their ability to proactively engage with the DPA and address DPA's concerns around issues of potential non-compliance.

The purpose of this paper is to:

- Inform the EU DPAs and the Article 29 Working Party as they consider the provisions of the GDPR on criteria to define the lead DPA and the co-operation among DPAs in the context of the OSS and the lead DPA
- Signal any practical challenges in implementing these provisions from the perspective of controllers and processors
- Suggest areas for further clarification in the forthcoming guidance from WP29

Finally, the EDPB consistency mechanism is not addressed in this paper. The complexity of that mechanism requires specific input by CIPL and will be dealt with in a separate paper.

[1] As explained in recital 127 GDPR. The substantive provisions of the GDPR do not mention the term "one-stop-shop".
[2] Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR), Adopted on 2 February 2016 (WP 236).

The CIPL GDPR Project

This paper is produced by the Centre for Information Policy Leadership at Hunton & Williams LLP ("CIPL") as part of its project ("CIPL GDPR Project") on the consistent interpretation and implementation of the GDPR.

The CIPL GDPR Project—a multiyear-long project launched in March 2016—aims to establish a forum for dialogue amongst industry representatives, the EU DPAs, the European Data Protection Supervisor, the European Commission, the ministries of the member states and academics on the consistent interpretation and implementation of the GDPR through a series of workshops, webinars, white papers and reports.

As part of the CIPL GDPR Project work plan for 2016, CIPL aims to provide input to the Article 29 Working Party ("WP29") on three of its priority areas: (a) DPO; (b) "high risk" and data protection impact assessments (DPIAs); and (c) certifications.

On 17 November 2016, CIPL issued a paper on the role of the DPO in the GDPR ("Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation"). The present paper fits within this series, giving input in a priority area of the WP29.

1. The importance of fully functioning OSS for consistent and effective implementation of GDPR

- **The promise of a true OSS is one coherent interpretation of the legal requirements, one single interlocutor, and legal certainty based on one regulatory process, one decision and one outcome.** These objectives should be preserved and considered at all times in the implementation of the relevant GDPR provisions by all stakeholders, including Data Protection Authorities ("DPAs").

- **Such a well-functioning OSS would be one of the most tangible benefits of the GDPR for all stakeholders concerned—organisations, DPAs and individuals**. In addition to obvious benefits for organisations operating across the EU, a properly executed OSS also strengthens the position of individuals by fostering a high level of protection across the entire EU and enables DPAs to be more effective by pooling expertise and resources, and by speaking with a single voice. A meaningful OSS would also contribute to the establishment and reinforcement of the Digital Single Market.

- **The lead DPA model enables "smart regulation"—it fosters an open and communicative relationship between the organisation and the DPAs; a deeper understanding of the organisation's business and data processing; and more effective supervision by creating better outcomes and encouraging more compliant behaviours**. The OSS avoids the burdens and inefficiency of managing multiple, sometimes conflicting, questions and requirements from DPAs. Instead, the OSS enables a streamlined communication channel between the organisation and the lead and one consistent interpretation of the law, whilst allowing any other DPA with an interest to still exercise oversight. It also enables organisations to develop meaningful working relations with the lead DPA, allowing this DPA to become more familiar with their business operations and their compliance history, thereby making the DPA's oversight more informed and enforcement more effective.

- **The OSS will bring changes to DPAs, organisations and individuals, which will require time, effort and evolving guidance and procedures.** DPAs will be most impacted by the new rules and new working procedures envisaged by the GDPR. With the GDPR imposing a duty for DPAs to contribute to the consistent application of the GDPR and co-operate with each other and the Commission (Article 51(2)), as well as the rules on co-operation and consistency in Chapter VII, DPAs will have to act and think both as European and national authorities. Organisations will have to consider proactively their relationship with relevant DPAs, including the lead DPA, as part of their data privacy compliance programs. Finally, individuals will have to understand the impact of the new rules on their rights under the law and how and where to exercise these rights. The amount of work and time needed to establish and evolve the new working arrangements and procedures in a way that meets the spirit of the GDPR must not be underestimated.

- **Dynamic yet coherent nature of guidance and procedures.** It is essential that any guidance, procedural arrangements and information to all impacted stakeholders are of a dynamic nature. They need to continue to evolve as all the stakeholders learn through practice. At the same time, it is important to ensure that guidance develops in a systematic, coherent manner with input from all relevant DPAs and industry, so that it preserves the policy goal of harmonising the law, its implementation and oversight across Europe.

- **The OSS process still has significant areas of uncertainty on how it will work in practice.** Particular areas where further guidance would be beneficial include a more concrete understanding of when the OSS will apply (i.e. the definition of 'cross-border processing'), the interaction with national laws, the process for designating the lead DPA, the organisation's relationship with other DPAs aside from their lead, the timing and process by which concerned DPAs notify the lead DPA of compliance concerns, the guidelines under which concerned DPAs will support the lead DPA's investigatory authority, and how to ensure that the redress mechanism as outlined in the GDPR does not undermine the very foundation of the OSS.

2. Transparency as a key requirement

- Transparency is **key for the functioning of the OSS**. The working arrangements, determining the co-operation among DPAs, should be fully transparent and based on clear and enforceable procedural rules.

- **DPAs should act in a transparent manner**, generally and vis-à-vis organisations. A well-functioning OSS requires not only that co-operation mechanisms work smoothly and in a meaningful way, but also that DPAs work transparently to ensure they are accountable to organisations and/or the general public for complying with their co-operation obligations. The relevant controllers and processors should also be notified without delay, via the lead DPA, about cases which concern them. Finally, individuals must understand the procedure in broad terms, too, in order to be able to exercise the rights under the GDPR.

- **Seamless and timely communication among DPAs** is indispensable if the OSS mechanism is to work effectively in practice.

- It will be also essential to maintain smooth **ongoing communication and co-operation between the lead DPA and the organisation** it supervises, including transmitting relevant information to

the organisations without delay. This will allow organisations to support more effectively the work of the lead and contribute to the efficiency of the process.

- This communication and co-operation would also **facilitate better and more targeted enforcement of the law**. Obviously, there are limits to transparency in ongoing investigations. However, these limits should be applied in a restrictive manner.

- Finally, we encourage **WP29 to create transparency tools** (information portals, automated notifications, schematic explanation of the procedures) and make those tools available for organisations and individuals concerned.

3. The designation of lead DPA

- It is clear from the text of the GDPR that each controller or processor will have one lead DPA, rather than multiple lead DPAs. Where a controller has taken steps to create a main establishment as defined in Article 4(16) or has a single establishment, the DPA in that jurisdiction shall be the entity's "sole interlocutor" (Article 56(6)).

- The GDPR simply states that the DPA of the main establishment or single establishment shall be competent (Article 56 (1). It is not yet clear how the **process for designating a lead DPA** will be managed. We would expect the controller or processor to be closely involved because the controller/processor is in the best position to identify where its central administration is located, or where decisions on the purposes or means of processing are taken (in the case of a controller), or where its main processing activities take place (in the case of a processor without a central administration). Organisations should be able to use their best judgement in this process, subject to assessment by the lead DPA.

- We would expect that DPAs offer some means for organisations to formally "register" with the lead. This "registration" would trigger the acceptance by the lead DPA to act in that capacity, and would inform other DPAs about the competence of the lead DPA. Guidance of the WP29 to this effect would be welcome.

- The current BCR approval process should provide insights and a precedent for the designation of a lead DPA. Organisations could be required to provide a written justification, supported by evidence, as to why their choice of lead DPA is appropriate. This justification could then be assessed by that DPA.

- Although the EDPB may issue a binding decision on who should be the lead in the event of a dispute, for certainty and ease of process we believe that the choice of lead should not be routinely subject to the approval of other DPAs. At most, upon information, there should be a quick and efficient procedure (subject to a deadline) permitting other DPAs to provide their views on the designation of the lead, with the goal of fostering consensus and avoiding the application of the dispute resolution procedure. The organisation concerned should also be able to address or rebut the views presented by other DPAs. Any alternative approach would lead to several months of uncertainty for the organisation concerned and thus should be avoided.

- In terms of **criteria** provided by the GDPR **for determining the main establishment**, we would suggest that there could be a third set of supplementary criteria applied, in cases where organisations **do not** have a formal central administration, do not determine the purposes and means of processing centrally (for controllers), and do not have a main place of processing

activities (for processors) either. In those cases, a more flexible set of criteria could provide an alternative, as discussed further in Section 4. For example, there could be a variety of factors, such as the EU entity of a controller/processor that has the most employees, or the greatest revenue derived from processing, or the majority of senior management, or the biggest growth plans, or the greatest volume of processing, etc. These are broadly consistent with the criteria used currently to determine the lead DPA in the context of BCR—a process that has been a marked success.

- We suggest that WP29 elaborates examples which would facilitate the application of these criteria for designation of the lead DPA in a more harmonised manner (see also Section 4).

- The GDPR (in particular Article 56(1)) suggests that the OSS mechanism and lead DPA is **mandatory** for organisations and applies by default, based on the existence of controller's or processor's main establishment in a member state and the existence of cross-border processing by that controller or processor.

- It is important that WP29 guidance clarifies that the designation of a lead DPA can take place any time, before or after the entry into force of the GDPR. In addition, an organisation should be permitted to periodically review the continued appropriateness of its lead DPA based on changed circumstances and discuss this with the lead DPA where appropriate.

- A final remark relates to organisations that currently have a main establishment in countries with similar laws as the EU, such as Norway and Switzerland, and—after Brexit—the UK, but that operate and have multiple establishments EU-wide. We encourage the WP29 to consider how these companies could in practice benefit from the OSS (including BCR approval process) and to ensure that the expertise of the DPAs in these countries will be taken into account or, in case of the UK ICO, will not be lost.

4. Determining main establishment and lead DPA

- One of the first steps for any organisation in the implementation of the GDPR will be to consider the application of main establishment criteria and the corresponding lead DPA as a single interlocutor for the purposes of GDPR oversight and enforcement. The application of Article 4(16), which defines main establishment for controllers and processors, raises some practical challenges for organisations which need to determine their main establishment in the EU and hence the lead DPA, as per Article 56 (1).

- It is clear that where a controller or processor is established only in a single member state, that member state DPA will be the lead DPA.

- Where a controller or a processor is established in multiple member states, the lead DPA will be the DPA of the main establishment (determined primarily based on the place of central administration, or secondarily where decisions on the purposes and means of processing are made (for controllers), or where main processing activities take place (for processors). This formulation may pose real challenges in practice for groups of companies operating in multiple member states, where the organisation comprises both controller(s) and processor(s).

    - This formulation raises the possibility of different main establishments—and hence different lead DPAs—for a single organisation that acts as both controller and processor. There are many organisations that provide IT or outsourcing services, and which may have

multiple establishments, but not a central administration in the EU. They may end up having one main establishment and one lead DPA in their role as a controller (based on where decisions about purposes and means of processing are made), and a different main establishment and a different lead DPA in their role as a processor (based on where main processing activities take place). Although recital 36 addresses some of these complexities by allowing for the lead DPA of a controller to be also the lead DPA for a processor, this interpretation seems to apply in cases of a controller and processor in two different organisations, but not as part of the same organisation. This should be clarified by WP29 to include cases where a single organisation acts as both controller and processor, so that in these instances an organisation can have a single lead DPA overseeing its processing activities as both a controller and a processor.

- It is quite feasible that in the absence of a central administration in the EU, a single controller may end up having a different main establishment for different types of data and processing (for example, employee data processing by HR and customer data processing by marketing), if decisions about purposes and means in respect of these two different types of data are made in two different EU countries. Organisations should be able to avoid this by having a single lead DPA for these cases based on the processing that the organisation believes to be more significant or prevalent.

- Some corporate groups are structured so that they have multiple controllers and multiple processors, all established and carrying out the same processing activities in different member states, rather than having a single controller or processor established in multiple member states. Based on the strict reading of Article 4(16), it would appear that these organisations would not be able to benefit from the concept of the main establishment, lead DPA and OSS, and would therefore be disadvantaged vis-à-vis other organisations. We believe that these organisations should be also allowed to determine their main establishment based on the criteria in Article 4(16) and recital 37, by explicitly allocating responsibility and decision making to a single dominant and influencing controller, or to a place of central administration, or alternatively by using the supplementary criteria we suggest in Section 3.

- It would be helpful if the WP29 guidance would confirm our understanding of the three situations above. It would also be helpful to clarify how organisations could benefit from the concept of the main establishment, lead DPA and OSS, in other situations where there is ambiguity regarding the identification of an organisation's main establishment in other concrete situations. While the primary intention of the GDPR is to designate a controller's or processor's central administration in the EU as the main establishment, this may not be applicable to all organisations. Although recitals 36 and 37 recognise the existence of complex business realities, these recitals do not solve all ambiguity, especially in situations where there is no central administration. It does not unambiguously determine the main establishment based on other criteria, or in situations of groups of undertakings (see recital 37). We suggest the WP29 consider supplementary criteria for those situations (closely linked to our suggestions in Section 3, for elaborating examples).

- The WP 29 guidance should confirm that the designation of a lead DPA in those cases should be based on a process with a true dialogue between the organisation and the concerned DPA(s). The organisation should have the possibility to express its views and propose what it considers to be its main establishment, and, as a consequence, how the OSS would be triggered. This is

essential since organisations are in the best position to understand their own business activities and management structures.

5. When does the OSS apply, and when will it be used?

- A fundamental issue in respect of the OSS is the interpretation of the concept of "cross-border processing" and its application by the DPAs in practice. A complaint by an individual in respect of his/her personal data (e.g. a rights request) may initially appear to be a matter reserved to the local DPA, on the basis that it only affects individuals in one member state. However, the position becomes less clear-cut when the complaint is in response to a position of the organisation which is applied across the EU and affects individuals in multiple member states. In this scenario, an organisation could be the subject of multiple complaints in different member states, all on the same issue, resulting in differing outcomes and undermining the OSS.

- By way of a specific example, an individual complains to a DPA in Hungary because a French media website has refused to erase his data in accordance with its EU-wide policy; this could be interpreted as purely a local issue, or it could be viewed as a cross-border issue on the basis that all individuals in all member states are affected by the *policy*. The ultimate disposition of the matter—if, for example, the company is instructed to amend its policy—will have an impact on that company's operations both in Hungary and potentially across the EU. Therefore, this situation would trigger the OSS.

- The GDPR ensures that even in local cases, DPAs notify the lead DPA without delay (see Article 56(3)). This notification mechanism could allow the DPAs to balance appropriately the local and a cross-border aspect. This notification mechanism should be effective and fully transparent in all cases (see also para 3).

- The lead DPA should take its obligation seriously, take on all cases which have cross-border implications, and put careful consideration into the decision to leave a matter to the local DPA. Cases which may initially appear to be only local may often have cross-border implications, which would not necessarily be obvious from only a brief consideration of the matter. It is crucial that the lead DPA consult the organisation as part of the complaints procedure.

- The WP29 guidance should address the application of the OSS in specific cases not explicitly mentioned in the GDPR. For example, we believe that the OSS should apply to: the notification of security breaches, when they affect individuals in multiple member states; requests for prior authorisation of high-risk processing with risks not being mitigated where such processing takes place in multiple member states; the approval of standard data protection clauses and contractual clauses (Article 46 GDPR); and the approval of BCRs.

- Finally, we note that Article 55(2) excludes the application of OSS and lead DPA for processing activities that are necessary for compliance with a local legal obligation imposed on a controller. In these cases, the competent DPA will be the DPA of a member state imposing the legal obligation in question. This may result in a situation where some processing activities, such as processing of personal data for the purpose of compliance with local anti-bribery laws, or anti-money laundering laws, are supervised by multiple DPAs, rather than a single lead DPA competent for all the other processing activities of the organisations' main establishment. The WP29 guidance should clarify these cases and indicate that these exceptions to the applicability of the OSS should be interpreted in a restrictive manner, in order to ensure a harmonised approach (see in this respect Section 3).

6. The OSS and organisations without an establishment in the EU

- The OSS does not seem to apply to controllers or processors not established in the EU in the situation foreseen in Article 3(2) GDPR. These controllers and processors must designate a representative in the Union (Article 27), who should be located in any of the member states where the individuals subject of targeting or monitoring are located. Equally, Article 56 (1) does not mention the situation of controllers or processors, without an establishment in the EU.

- The guidance of the WP29 should clarify whether the foreign controllers and processors in Article 3(2) can benefit from the OSS and the lead DPA.

- We also suggest that this guidance clarify if a company which has an establishment in the EU for some of its business activities, but not for all of those activities, should be able to benefit from the OSS for all of its activities. This would avoid unnecessary complexity for companies and, more generally, would ensure the widest possible application of the OSS.

7. How will the DPAs work together to ensure the OSS functions effectively as a means of allowing input by all DPAs, but still resulting in a single decision?

- Article 60 of the GDPR aims to ensure an efficient and timely decision-making process. It is thus imperative that the timelines provided therein (and elsewhere) are respected by the DPAs, ensuring that the OSS mechanism does not cause major delays in the approval/decision-making process.

- Timely decision making is core to the respect of the fundamental rights to privacy and data protection. Individuals and organisations have the right to receive a decision within a reasonable timeframe, and within the timeframes specified in the GDPR. It is essential that the specific timeframes for review and revisions to be made in relation to a draft decision are respected. The lead DPA is granted considerably leniency in terms of timeframes (for example, no specific timeframes are given for submitting the first draft decision to the concerned DPAs, submitting a matter to the EDPB or adopting a final decision). Nonetheless, there should be an expectation that lead DPAs will act with due expediency to avoid undermining the other timeframes specified in the GDPR.

- We are also concerned about the procedural aspects, timelines and efficiency in the situations where a lead DPA has to co-operate and consult with all other 27 EU DPAs, as there will be many cases where all 27 DPAs will be considered concerned DPAs because individuals in all member states are affected (or there have been complaints in all member states). Maybe these truly pan-European cases could warrant use of a smaller group of concerned DPAs that would work with the lead DPA. Such smaller group could be composed through a rotation process that would ensure a fair workload distribution in such cases across all concerned DPAs. The current BCR approval process with a lead DPA, two other DPAs and the process of mutual recognition again provides a useful precedent for such cases. We suggest the WP29 consider such a representative mechanism to deliver efficient decision making and avoid unnecessary substantive involvement by all concerned DPAs, especially in cases with urgency, or cases that do not involve high risk.

8. How will the lead DPA's investigation interact with national law in different member states?

- The GDPR interacts at numerous instances with national law. This interaction will be relevant to cross-border processing. For instance, in situations where individuals are located in member states other than the member state of the main establishment, the lead DPA may be required to apply the law of another member state. In short, in many instances applicable law will not coincide with DPA competence under the OSS, e.g. the law of the lead DPA. A concerned DPA will have to ensure that, where appropriate, its national law is considered in the decision-making process by a lead DPA.

- However, it should be ensured that in cases where the GDPR and national law simultaneously apply, an organisation can indeed rely on its lead DPA to apply the OSS, with the involvement of other concerned DPAs. We should avoid the OSS's being undermined by multiple parallel DPA investigations on the basis of national law. The provisions in Article 60(1) obliging concerned DPAs to exchange all relevant information and to provide mutual assistance to the lead authority under Article 61 support this view of the lead as the single central investigator. Parallel investigations should not be permitted, save in the limited circumstances where a "joint operation" occurs under Article 62.

- There are numerous examples when *both* national law and the GDPR will apply. In these circumstances, the lead DPA will take into account the national laws of other member states where an organisation is also established. This could result in a situation where a DPA decides an organisation has not breached the GDPR but has breached the national law of *another* member state.

- As much as possible, organisations should be able to utilise their lead DPA, and not be subject to an OSS investigation *and* parallel investigations by other DPAs who consider their national law to be engaged. However, guidance is needed to ensure that in situations where the GDPR applies simultaneously with national law, including the national law of member states other than the member state of the lead DPA, efficient and quick procedures are applied. A decision of a lead DPA should also clearly demonstrate how it dealt with this accumulation of applicable law.

- **At the heart of the OSS mechanism is a desire for a consistent interpretation of data protection laws across the EU. The fact that concerned DPAs can be part of the OSS mechanism means that the OSS provides for an ideal mechanism to also address issues where national laws are engaged and find a compromise between the position of all those concerned.**

- Here are some examples from the GDPR to put this discussion in context:

    a. Scenario 1: A breach solely of national law: An organisation processes genetic data across the EU in a manner which is compliant with the GDPR, but breaches further conditions laid down by multiple member states under Article 9(4).

    b. Scenario 2: A breach of both national law and the GDPR: An organisation processes genetic data across the EU in a manner which breaches *both* the GDPR and the further conditions laid down by member states.

    c. Scenario 3: A breach of the GDPR by reason of national law: An organisation processes personal data of children without obtaining parental consent for children over age 14.

Some member states have chosen to reduce the age of consent to 13, hence this is a breach of the GDPR only in some countries.

- In light of the significant scope for overlap and fragmentation between national law and the GDPR, it is essential that there be a process to allow for one interpretation of the applicable standards, facilitated by the lead DPA. Where there is a divergence under national law, it will be *particularly* important for the lead DPA to work with the other concerned DPAs to agree on a single interpretation.

- **Provided the lead DPA has involved the other concerned DPAs and taken due account of their comments, it should be clarified that those other DPAs must accept the single decision and cannot launch investigations—even under their national law**.

- The role of the national courts in the event of an appeal against the DPA's decision is also unclear in these circumstances (as well as more broadly, as explained below in Section 11). The right to appeal under Article 78 applies even where there has been an escalation to the EDPB. This again raises questions regarding applicable law. If the lead DPA and/or the EDPB took into account the views of other DPAs (based on their national law, or interpretation of EU law), the national court will be obliged to consider other national laws, to the extent these are applicable to the processing.

9. When will a "concerned DPA" have jurisdiction?

- Article 4 (22) GDPR gives a definition of "supervisory authority concerned". This definition encompasses three situations: having a controller or processor established in the member state of the DPA; individuals in that member state are/are likely to be substantially affected; a complaint has been lodged with the DPA.

- This definition is only used in a substantive provision of the GDPR in relation to the co-operation with the lead DPA in the context of the OSS mechanism (Article 60). It should be clarified in WP29 guidance that the definition of "supervisory authority concerned" does not create jurisdiction vis-à-vis a controller or processor, also in other contexts. To be more precise: There is no DPA jurisdiction outside its border. A complaint can be handled "locally", only in situations of Article 56(2). In other situations, the OSS should be triggered when there is a complaint.

10. What will the organisation's relationship be with other DPAs?

- Although the GDPR is clear that the lead DPA should be the "sole interlocutor" in relation to cross-border processing (Article 56(6)), we anticipate that the other DPAs may still want to maintain a relationship with organisations, even when they are not the lead. Equally, some organisations may wish to engage proactively with these DPAs, for example to pre-empt misunderstanding, or possible investigations.

- However, it is not clear how the DPAs will apply the restriction in Article 56(6) in practice. Would this, for example, prevent *any* dialogue directly between an organisation and other DPAs with respect to cross-border processing (e.g. to discuss a particular project or product launch)?

- Although it is very helpful to have a single point of contact, we do not think this should be interpreted too rigidly. Organisations should be allowed to have informal dialogue, co-operation and consultation with other DPAs, in addition to lead DPAs, if they wish to do so. In fact, the

specific tasks of the DPO provided in Article 39(1)(d) and (c) are to co-operate and consult with DPAs, which would include both lead DPA and national DPAs, given that the DPO can be appointed for a group of companies, or at national level. We note that the group DPO does not have to be located in the country of the main establishment or lead DPA.[3]

11. What happens when a complaint is only partially dismissed, so that any challenge must be conducted in separate courts?

- Articles 60(8) and (9) provide that where all or part of a complaint is ***dismissed***, the decision is adopted by the DPA to which the complaint was made. In the case of a partial decision, any parts of the complaint which are ***upheld*** will be made by the lead DPA. A potentially significant difficulty could arise here in the event of an appeal against a complaint which has been only partially dismissed. Under Article 78, any appeal against a DPA decision should be brought in that DPA's member state. Accordingly, a scenario could arise where part of a complaint is rejected, and an appeal begins in Member State A, whilst part of a complaint is upheld, and an appeal begins in Member State B (and potentially many other countries). This could seriously undermine the core objective of the OSS mechanism: one legal process, one outcome, one coherent interpretation of the EU law.

- The courts have discretion to suspend proceedings or decline jurisdiction under Article 81, but this is only a *discretion* (and the courts may take a view that they are sufficiently separate issues). This could therefore lead to differing court decisions and analyses in respect of a single complaint—albeit one covering various different points of law.

- Furthermore, it seems unlikely that, in a case of cross-border processing, an investigation would be prompted by only one complaint. It is more likely that complaints will be received by multiple DPAs, and these will be consolidated into one investigation—facilitated by the lead DPA. In the event that these complaints are dismissed by a *single decision through the OSS*, there will nonetheless be multiple "final" DPA decisions. Consequently there could be appeals in multiple member states. Under Article 81(3), whichever court was seized first can decline jurisdiction, but again this is only a discretion.

- To the extent that the OSS can provide a solution to the problem of multiple parallel proceedings, strenuous efforts should be made by the DPAs (both lead and concerned) to do so. The purpose of the GDPR, and in particular the OSS, is to provide for a uniform application of the law across the EU and avoid parallel and sometimes conflicting proceedings in different member states.

- We invite the WP29 to include in its guidance the different scenarios of parallel proceedings, and options for dealing with these scenarios, including the role of preliminary rulings by the Court of Justice of the EU.

12. Harmonisation of DPA powers

- Article 58(6) allows member states to provide in national law for additional powers of DPAs. These additional powers should not impair the effective operation of the OSS, co-operation and consistency mechanisms.

[3] See CIPL Paper on "Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation" at p. 20.

- CIPL takes the view that member states must be discouraged from providing additional powers to DPAs, as that may adversely affect the operation of the OSS. Some DPAs will feel they have more powers then others and may resist the OSS and handing over competences to the lead DPA, where such DPA would not have the same powers. Differentiation in powers may diminish the trust in the OSS mechanism. Additional powers are also not needed, in view of the long list of DPA powers included in Article 58 GDPR.

13. The urgency procedure should not undermine the OSS

- Although this paper does not address the consistency mechanism, CIPL wishes to note that there might be a risk that the urgency procedure of Article 66 GDPR is invoked in situations where this is not strictly necessary, undermining the OSS. It should be ensured that the urgency procedure is invoked only in exceptional circumstances. Provisional measures adopted by supervisory authorities should be well-founded in law.

- Article 66 indicates that supervisory authorities may invoke the urgency procedure when there is an "urgent need to act in order to protect the rights and freedoms of data subjects". In addition to the process outlined in Article 66, we suggest that DPAs consider a number of supplementary factors in deciding whether to invoke this measure in order to maximise the goal of quickly resolving potential threats to data subjects' rights and freedoms.

- In this paper we just raise this issue to WP29's attention, so that it can be further considered in the context of guidance on the consistency procedure.