Centre for Information Policy Leadership
Hunton & Williams LLP

15 February 2017

**Comments by the Centre for Information Policy Leadership**

**on the Article 29 Data Protection Working Party's**

**"Guidelines for identifying a controller or processor's lead supervisory authority"**

**adopted on 13 December 2016**

On 13 December 2016, the Article 29 Data Protection Working Party (WP29) adopted its "Guidelines for identifying a controller or processor's lead supervisory authority" (guidelines) and associated Frequently Asked Questions (FAQs). The WP29 invited public comment on the guidelines by 15 February 2017. The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to submit the brief comments below.

These additional comments follow up on CIPL's 30 November 2016 white paper on *The One-Stop-Shop and the Lead DPA as Co-operation Mechanisms in the GDPR* (CIPL White Paper), which contained CIPL's initial input to the WP29 guidelines.[2]

In the CIPL White Paper, we underlined 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. We also stressed that this new mechanism can only become a success if there is sufficient clarity on the meaning of the relevant GDPR concepts, as well as on their implementation. In addition, it bears mention that the OSS was originally designed to reduce administrative burdens for companies resulting from having to deal with divergent rules and practices of different DPAs, which is even more important given the harmonised rules under the GDPR. Any guidelines on the OSS should keep the principle of harmonisation as a main guiding thread to avoid creating even more uncertainty and inconsistency than exists under the current Directive.

CIPL welcomes the WP29 guidelines as generally well-balanced and pragmatic and helpfully clarifying a number of issues in relation to the cross-border processing of data and the lead

[1] CIPL is a privacy and data protection think tank in the law firm of Hunton & Williams LLP and is supported by approximately 50 member companies that are leaders in key sectors of the global economy as well as by additional companies that are participating in issue-specific CIPL projects. CIPL's mission is to engage in thought leadership and develop best practices to ensure effective privacy protection in the modern information age. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Note that nothing in this submission should be construed as representing the views of any individual company supporting CIPL or participating in CIPL's projects or of the law firm Hunton & Williams.

[2] The CIPL White Paper can be found at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_the_gdpr_one-stop-shop_30_november_2016.pdf

supervisory authority. We especially welcome that this guidance is given in this early stage, making it possible for companies to prepare for the new legal regime.

CIPL also welcomes that the guidelines provide for a central role for organisations in the process of designating the lead DPA. This is fully in line with the views expressed in the CIPL White Paper that the controller or processor should be closely involved in the process for designating a lead DPA, because the controller/processor is in the best position to identify where its central administration is located, or where decisions on the purposes and means of processing are taken, or where its main processing activities take place.

The guidelines should be regarded only as a first step towards a fully functioning OSS, as some of the key concepts therein require further specification.

We suggest that the WP29 consider the guidelines as a living document. Accordingly, the guidelines should be regularly updated in the near future, based on consultations with stakeholders and the initial experiences once the GDPR comes into effect.

## Comments

1. Identification of the lead DPA (pp. 6-7)

The guidelines explain that the controller/processor identifies where its main establishment is and therefore which supervisory authority is its lead DPA. This can be challenged by the respective supervisory authority concerned afterwards.

This distribution of roles is fully in line with, on the one hand, the starting point that DPAs should rely on the organisation's own expertise[3] and, on the other hand, the statement by the WP29—fully supported by CIPL—that the GDPR 'does not permit forum shopping'.[4]

We suggest that the guidelines clarify that this distribution of roles as a starting point for the OSS applies to all situations where the lead DPA needs to be identified. The current text may lead to confusion since this important explanation is included in the section on groups of undertakings.

Moreover, the guidelines helpfully mention the specific situation where a controller established in multiple member states does not have a central administration in the EU and none of the EU establishments decide on the processing. For pragmatic reasons, such a controller is entitled to designate the establishment that will act as its main establishment.[5] This pragmatism, which

[3] This is a central notion in CIPL's White paper. See, in particular, at 2.
[4] Page 7, Section II, para ii, of WP 29 Guidelines.
[5] Page 7, Section II, para ii, of WP 29 Guidelines.

enables organisations not only to identify, but even to determine the lead DPA, should be guiding in all situations where the GDPR does not give a clear answer on who should be the lead DPA.

**Recommendation: State in a more explicit manner and applicable to all situations that the functioning of the OSS is based on the identification of the lead DPA by the organisation itself (the controller or the processor), subject to review by the DPA based on all relevant facts. Moreover, in view of the complex realities, pragmatism should be guiding in all situations where organisations seek to determine the lead DPA and the application of GDPR requirements is not sufficiently clear.**

2. Groups of undertakings (pp. 6-7)

The guidelines touch upon the processing by a group of undertakings and explain the identification of the lead DPA where, within a group of undertakings, one establishment can be considered the overall controller for the entire group. This is in line with the last sentence of Recital 36.

In many situations, however, a group of undertakings will be organised in a way that it cannot be considered as one controller and, hence, prima facie not benefit from the OSS mechanism. This is for instance the case when, within a group, each legal entity controls the nature and purpose of the processing and as a consequence each entity is regarded as a controller in respect of similar types of processing. However, even if there are multiple legal entities, if the nature of the processing and/or issue is identical across the entire group, the group may benefit from the OSS, if only for reasons of effectiveness. An example of this might be the situation where multiple entities in a group contract with a processor under a single service agreement; if an issue were to arise in relation to that agreement, it would surely be logical for any investigation to be led by the group's lead DPA under the OSS.

Moreover, groups may also be organised in a way that the parent undertaking is the controller for some data sets, whereas other data is controlled at the level of the individual entity – for example, if an entity carries out direct marketing under its own brand name it will often have control of any marketing data and no other member of the group will have such control. Equally, there are cases where two or three companies in a group share a data set but no other companies have access to it.

In brief, the nature and level of control in groups of undertakings is very diverse. In view of this diversity and complexity, CIPL welcomes the flexibility in the guidelines (p. 7). In the case of a group of undertakings the parent undertaking cannot always be regarded as the controller for

the group. If other entities in the group have real control and decision-making over personal data, they should be treated as the relevant controllers. However, we suggest to further develop examples of different situations which would be helpful as practical guidance. We refer in this specific context to the examples included in Section 4 of the CIPL White Paper.

**Recommendation: Elaborate on the different realities of controllership within groups of undertakings and the consequences for the identification of a lead DPA and provide practical examples.**

3. Process of designating a lead DPA (pp. 7-8)

It would be helpful to give a general indication of the steps involved in the process of designating the lead DPA, including indicative time frames. The process already established in the BCR context could serve as example. Giving a general indication is important to enhance legal certainty for organisations, as well as for the accountability of all involved.

We note in this context that the guidelines assert that 'conclusions cannot be based solely on statements by the organisation under review' and 'the burden of proof ultimately falls on controllers and processors.' While we agree that mere declaration by the organisation cannot be the sole basis for the designation of the lead DPA, we would like to underline that the text of the GDPR does not assign any burden of proof to controllers or processors. An assessment should be based on objective factors. A supervisory authority may rebut the assertions of a controller or a processor on the basis of an examination of the relevant facts, where possible in an open collaboration with the controller or processor concerned.

Moreover, the process of co-operation between businesses and supervisory authorities in the designation of the lead DPA should be elaborated in the guidelines, ensuring consultation of organisations in the designation process.

**Recommendation: Specify in more detail the process of designating a lead DPA and how it will be managed, in line with Section 3 of the CIPL White Paper.**

4. The OSS and local issues

    a. Supervisory authority concerned (p. 8)

The guidelines address the situation of Article 56, paragraphs (2) and (5) GDPR providing for a concerned supervisory authority to take a role in dealing with a case without being the lead supervisory authority.

This is explained by an example of a French company launching a product only in Portugal. This example is an illustration of a purely 'local' processing, which is cross-border by virtue of the location of the controller. This is an area where greater clarity would be helpful. The guidelines explain that, in accordance with Recital 127, the lead DPA may decide this situation should be handled by the local DPA.

However, it would be helpful if controllers were given the opportunity to give input in this decision. One can imagine several circumstances where an issue initially appears to be purely local, but which subsequently arises in multiple member states. To provide an example, an individual in Germany complains that his access request has not been properly dealt with by a Hungarian controller. This could initially appear to be a purely 'local' issue and handled by a German DPA (as it concerns only one individual); however, if the controller's actions reflect a companywide practice (instead of a one-off incident), it could affect individuals in multiple member states and it is not unlikely that complaints from individuals in other member states would follow.

Accordingly, we would recommend the lead DPA be sensitive to this possibility, and exercise caution before giving up its role as the lead. We anticipate that the lead DPA will generally be best placed to exercise its powers.

We would also welcome clarification that the OSS will still apply where the processing affects data subjects in more than one member state, even if those data subjects are not located in the jurisdiction of the lead DPA (e.g. if, in the example in the guidelines, the product was only launched in Portugal and Spain).

Finally, it is unclear on what basis the local DPA would have jurisdiction over the controller, in a situation where it was not established in that member state.

**Recommendation: <u>Elaborate on the decision-making process when a lead DPA may give up its role to a concerned DPA, and specify that controllers will be given the opportunity to provide input into this decision. Moreover, the guidelines should encourage DPAs to exercise caution in this regard, recognising that, generally, the lead DPA will be best placed to exercise its powers</u>.**

5. <u>Transparency (p. 8)</u>

    a. Transparency should be the rule

Point 4 of the CIPL White Paper underlined transparency as key for an effective OSS. This also includes an open dialogue and co-operation between businesses and authorities. Further, the

co-operation between the lead DPA and concerned DPAs should be fully transparent, enabling organisations to give their views, where needed. This transparency should be the rule, while acknowledging that there are limits, due to the need to retain confidentiality in the interest of the effectiveness of data protection enforcement. However, confidentiality should be the exception and be limited to situations where this is necessary. The guidelines should explicitly address this.

Organisations should be able to understand how the lead authority and the concerned DPAs co-operate. As a principle, the positions of the various DPAs should be available for the organisations. For example, it may be helpful to share with the controller or processor concerned the assessment of a situation in the light of the fundamental rights and the CJEU's case law, clarifying the perspectives of (all) the concerned DPAs. The guidelines might also suggest specific means for facilitating an open exchange of views between concerned supervisory authorities and the relevant controllers and processors.

**Recommendation: Explicitly state in the guidelines that the co-operation between the lead DPA and concerned DPAs should be fully transparent, enabling organisations to fully co-operate, where needed, respecting the interest of effective enforcement.**

b. Reference to the EDPB

The guidelines (p. 8) mention the reference to the EDPB where DPAs have conflicting views regarding the identification of the lead DPA. CIPL suggests that organisations should be given the opportunity to present their positions and views in this procedure, possibly as part of the reference to the EDPB.

**Recommendation: Specify that organisations will be given the opportunity to present their positions and views in the procedure of referring a matter to the EDPB.**

6. The lead DPA and processors (p. 9)

a. The processor and the OSS

The guidelines simply repeat Recital 36 which states that in cases involving both the controller and processor, the competent lead authority will be the lead authority for the controller and the decisions of the lead DPA of the controller will be binding on the processor. Hence, there will be one lead DPA for both the controller's and processors' activities.

As indicated in the CIPL White Paper, it is not quite clear what situations are covered in the GDPR's Recital 36. The guidelines do not add any further clarity to this point either. Does the

recital cover a situation where a single organisation acts as both a controller and a processor in respect of different data processing? Or does this recital only relate to a cross-border case that involves both a controller and a processor, where they are separate organisations and a lead DPA has to be determined?

**Recommendation: Address explicitly both situations mentioned above and clarify the position in both cases.**

b. A processor acts on behalf of multiple controllers

Recital 36 and the guidelines might pose a problem when a processor processes personal data on behalf of multiple controllers in different member states, such as large cloud service providers, or IT or outsourcing providers. In these situations, if we interpret that the lead DPA will be that of each controller as implied by Recital 36, there is a risk that processors will not be able to benefit from the OSS and may be confronted with inconsistent enforcement actions (in addition to having a separate lead authority responsible for processing for which the company is controller, i.e. processing of employee personal data). In practice, this may be a huge hindrance for large-scale processors and such an interpretation would not be in line with a key objective of the GDPR.

In the case of a processor delivering services to multiple controllers in EU, the main establishment of the processor should be the place of its central administration, or, in the absence of a central administration, where the majority of processing activities take place, as provided by the GDPR. Naturally, the processor, just like the controller, will determine where that location is, subject to DPA review.

**Recommendation: Clarify that a processor acting on behalf of multiple controllers may determine its lead DPA pursuant applicable GDPR requirements subject to DPA review, thus making it possible for processors to benefit from the OSS.**[6]

c. The controller does not have any establishment in the EU

Another situation that needs clarification is where a controller does not have any establishment in the EU—and hence does not benefit from the OSS—but uses a processor operating in different member states with a main establishment in one of the member states.

[6] In addition, as discussed on pp. 6-7 of CIPL's white paper on the OSS (see above p. 1), in cases where a group of organisations comprises both controllers and processors or a single organisation acts as both controller and processor, it should be clarified by the WP that an organisation can have a single lead DPA overseeing its processing activities as both a controller and processor.

We believe—on the basis of a combined reading of Recital 36 and Article 56—that if the non-EU controller does not have a lead DPA, the supervisory authority of the processor could be the lead DPA in respect of the processor, provided the processor is able to determine a main establishment as set out in Recital 36.

Furthermore, the guidelines should make it clear that a processor with a main establishment benefits from the OSS mechanism also in situations where the GDPR applies to a non EU-controller on the basis of Article 3(2) GDPR. Obviously, in this situation the lead DPA would only be competent in relation to the processor and not in relation to the controller.

**Recommendation: The situation of a processor acting on behalf of a controller not established in the EU should be clarified in the guidelines, making it possible for processors to benefit from the OSS.**

d. In general terms, processors should benefit from the OSS

Article 56 (1) of GDPR confirms that processors can benefit from the OSS. Therefore, the guidelines should be clarified to avoid the consequence for a processor of not being able to benefit from the OSS. In short, CIPL suggests the WP29 elaborate on this issue further in the guidelines, to provide for a mechanism for processors to flag practical problems with their own lead DPA or with the EDPB, and, most importantly, to ensure that these practical problems, when justified, are solved within the consistency mechanism.

**Recommendation: Address the need for processors to fully benefit from the OSS and offer practical solutions for cases in which processors serve multiple controllers in different member states and the controllers do not have a lead DPA, as well as where a single organisation acts as both controller and processor, with potentially different main establishments. The same applies where the controller does not have an EU establishment, but the processor has.**

e. The concept of 'main processing activities'

In situations where the processor is not able to determine a place of central administration in the EU, the guidelines should confirm that the location of the 'main processing activities' simply refers to the location in the EU where the majority of data processing of the processor takes place. This could, for instance, be the location of the largest data or IT delivery center, hosting customer/client data or delivering client services.

**Recommendation: The guidelines should clarify the notion of main processing activities.**

7. The lead DPA and joint controllers

The guidelines do not address the case of joint data controllers. Guidance is needed to determine the lead supervisory authority in the situation where joint controllers have their main establishments in different jurisdictions, in line with the obligations of the joint controllers in Article 26 GDPR. This guidance should take into account the general requirements for designating a lead DPA, in particular the place where the means and purposes of the processing are determined.

Under the GDPR, joint controllers may have different lead DPAs depending on their own main establishment. CIPL suggests that where there are two (or even more) lead DPAs for joint controllers in respect of the same processing operation, these lead DPAs should co-operate more closely and endeavour to take a common position. This is a situation where divergence needs to be avoided per se. Hence, where needed, the consistency mechanism should be invoked.

**Recommendation: Provide guidance for the case where the joint controllers have their main establishments in different jurisdictions and to ensure effective co-operation between the competent lead DPAs and, where needed, invoke the consistency mechanism to avoid a situation which may lead to legal uncertainty.**

8. Location of a central administration and the place where decisions on means and purposes of data processing are taken (p. 5 and p. 7)

    a. The main establishment is not the location of the central administration in the EU.

The guidelines do not make a clear difference between the 'location of a central administration' and 'the place where decisions about purpose and means of data processing are taken'. For instance, they state (p. 5) that 'the central administration in the EU is the place where decisions about the purposes and means of the processing of personal data are taken.'

The distinction should be made clear, beyond the factors included on page 7 of the guidelines, which are meant for cases where the main establishment is not the location of the central administration in the EU. In CIPL's view, if an organisation has a central administration or headquarters, that should by default be the main establishment. However, an organisation may be organised in a way that the 'decisions about the purposes and means of the processing' are taken elsewhere. In that case, this will determine the main establishment, because the place where decisions are made is in the specific case more important than the formal seat of a

central administration. This reasoning should be accepted, provided it is sufficiently supported by facts.

We take the view that, as a rule, even if there is no clear entity with overall control, that the overall decision-making center within an organisation (based among others, on the criteria on page 7 of the guidelines) should be the single or main establishment for the organisation. Assessing the main establishment for each legal entity or processing activity would run completely against the concept of the OSS, because it could lead to organisations' with different activities located in various member states having numbers of main establishments.

This would also make it more difficult for an organisation to have a strong central DPO team with oversight over all aspects of the group and to manage the relationship(s) with the lead DPA. It would also make it more challenging for supervisory authorities to engage with an organisation where a data protection issue spans across several business activities and/or legal entities.

Similarly, it is not clear how to deal with the situation where the central administration determines the means and purposes of the processing, but where an affiliate adjusts the processing to comply with local specificities. The WP29 should make clear that local adaptation based on specific national requirements of general policies set by the central administration does not change the outcome of the determination of the main establishment.

**Recommendation: <u>Clarify further the difference between place of central administration and the location that determines the means and purposes, and specify requirements for both, based on the objectives and principles underlying the OSS. Moreover, make clear that local adaptation based on specific national requirements of general policies set by the central administration does not change the outcome of the determination of the main establishment</u>.**

b. Establishments organised per product line or business line.

To make it even more complicated: In many organisations, the business decisions (and, thus, the processing activities inextricably linked thereto) are not adopted by an 'establishment' but rather by global and/or regional groups within the company that are composed of individuals, who are employed by different establishments in the EU or elsewhere. These individuals are not representing an establishment or determining a member state's jurisdiction, but they rather represent a business line or a product line, or the whole business activity of a specific geographic region. In the vast majority of cases, however, it would still be logical for the organisation to have a single lead DPA. This would allow for a greater level of consistency, and

avoid the need to establish a new process to enable two lead DPAs to work together, in the event of an issue affecting the organisation as a whole.

We suggest that the guidelines should add a scenario in which the 'central administration' is organised per product line or business line and not per geographical entity, office or location. So, for example, the Paris entity of a company could house the central administration of two product lines (e.g. phones) and the Berlin entity could house two different lines (e.g. laptops). We argue that it is possible to look at companies through the lens of product and business lines and determine the central administration on that basis. So, in the example above, the lead authority for phones would be the French DPA, but for laptops it would be the competent German DPA.

We believe that the best solution for these types of scenarios is to recognise in the guidelines that the group of undertakings should have the flexibility to decide whether one main establishment or several (per business line) are appropriate based on how decisions are being undertaken and other relevant factors.[7]

**Recommendation: Clarify that in cases where the central administration may differ between different product and business lines, organisations should be granted flexibility in deciding whether one or several main establishments are appropriate, based on how decisions are made and other relevant factors. Clarify further how multiple lead DPAs may work together in those cases where a decision resulting in multiple lead DPAs for different product or business lines is made. In all cases, the organisation should be allowed to present its views.**

9. OSS and data transfers

a. *Schrems* revisited

Obviously, when the jurisdictions of two or more EU member states are concerned, the OSS mechanism will also be relevant in the context of data transfers outside the EU. In respect of mechanisms for cross-border transfers, the controller or processor has to deal only with the lead DPA as the sole interlocutor (Article 56(6) GDPR).

We suggest the guidelines clarify that once the GDPR is fully in force, the use of independent enforcement powers of each national DPA doesn't require each of them to check each cross-border transfer with due diligence (for instance in case of a complaint), as required by the CJEU in the *Schrems* case, since this will be the task of the lead DPA.

[7] Also, we suggest that guidelines include the various situations addressed in Section 4 of CIPL's white paper (pp. 6-7) relating to the establishment of a lead DPA for organisations operating in multiple member states as both controllers and processors.

**Recommendation: <u>Confirm that the assessment of data transfers based on due diligence, as required in the *Schrems* judgement, will now be primarily a task of the lead DPA</u>.**

b. Earlier assessment in the context of BCR should still play a role

The guidelines do not refer to BCR, nor to the well-established and useful criteria that have been used to determine the lead DPA for the purpose of BCR approval procedures. We recommend that the WP29 confirm that the assessment of a lead authority carried out in the context of the BCR will still be relevant and can play a role in identifying the main establishment and lead DPA under the GDPR.

We also suggest that the criteria included on page 7 of the guidelines are augmented by additional criteria used to determine the lead DPA for the purpose of BCR approval.

**Recommendation: <u>To confirm that the identification of a lead authority carried out in the context of the BCRs will play a role in identifying the main establishment and lead DPA under the GDPR</u>.**

10. <u>In general: more examples are needed (p. 7 and annex)</u>

The guidelines provide helpful examples of cross-border processing. However, in view of the many different possible factual scenarios, including in the context of groups of undertakings, in which decisions about data processing are taken at different levels, we suggest adding an annex to the guidelines with examples for such different scenarios. The guidelines would be more practical and valuable if they provide more practical examples, to be used by organisations to help determine the lead DPA. If needed, this can be done or continued at a later stage based on initial experiences.

The examples where OSS and lead DPA will kick in should include both contentious and non-contentious scenarios. This is important in order to make it clear that the OSS applies not only in the case of enforcement, complaints and investigations, but in respect of other provisions of the GDPR requiring interaction with DPAs, including prior consultation in limited cases of DPIAs, BCRs and other data transfer mechanisms, security breach notifications, etc.

Furthermore, it would be helpful to have examples to clarify the cases where the decisions on the purposes and means are not taken in the place of the central administration of the controller, giving practical meaning to the bullet points on page 7 of the guidelines. This includes, for instance, the factors determining the main establishment, when it is not the same as the location of a company's central administration.

**Recommendation: <u>Add an annex to the paper with explanatory examples for different practical situations</u>.**

## Conclusion

Thank you for the opportunity to provide further comments on key implementation questions in relation to the lead DPA and the OSS. To the extent the WP29 decides to accommodate all or some of our suggestions, we would assume you would also update the associated Frequently Asked Questions. We look forward to providing further input on the OSS Guidelines in the future as new issues arise, particularly in light of any practical experiences in applying the GDPR. In the meantime, please do not hesitate to contact us for further information or clarification at bbellamy@hunton.com; mheyder@hunton.com; and hhijmans@hunton.com.