18 January 2019

Comments by the Centre for Information Policy Leadership
on the European Data Protection Board's
"Draft Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)"
Adopted on 16 November 2018

On 16 November 2018, the European Data Protection Board ("EDPB") adopted its Draft Guidelines on the territorial scope of the GDPR (Article 3) ("Draft Guidelines").[1] The EDPB invited public comments on this document by 18 January 2019. The Centre for Information Policy Leadership ("CIPL")[2] welcomes the opportunity to submit the comments below as input for the EDPB's final Guidelines ("Final Guidelines").

Comments

CIPL welcomes many of the clarifications provided by the Draft Guidelines as a basis for the consistent application of Article 3 of the GDPR. The Draft Guidelines confirm the common interpretation of the territorial scope of the GDPR. It is also helpful that the Draft Guidelines include many concrete examples. This will help put an end to much uncertainty for organisations, data protection authorities ("DPAs") and other stakeholders on a number of questions, including several situations where the GDPR's application appeared unlikely at first glance. Clarity as to whether an organisation is subject to the GDPR is a prerequisite for consistent and effective GDPR compliance by controllers and processors.

At the same time, however, CIPL identified situations where the Draft Guidelines stretch the criteria triggering the application of the GPDR too far, resulting in overlap and sometimes conflict of national laws. This leads to further complexity, particularly for organisations operating both in the EU and outside of the EU, whether they have an "EU establishment" or not. CIPL elaborates on these cases below, providing comments for each section of the Draft Guidelines.

Furthermore, CIPL respectfully suggests that the EDPB address the relationship between Article 3 on territorial scope and Chapter V of the GDPR on international transfers as both topics are closely related. This could be done through future subsequent guidelines. Such guidelines should be drafted without delay so that it doesn't postpone the release of the Final Guidelines on territorial scope.

Moreover, CIPL recommends that the Final Guidelines be adjusted to reflect the application of Article 3 in the European Economic Area ("EEA") where such countries are considered to be

[1] Draft Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf.

[2] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth and is financially supported by the law firm and 70 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 at http://www.informationpolicycentre.com/. 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.

"Member States" for the purposes of the GDPR[3] as the Draft Guidelines currently mention only the EU and not the EEA.

In general, given the complexity of the real-life application of Article 3, across multiple scenarios, CIPL believes that more clarity is needed as a whole with regards to the extraterritorial applicability of the GDPR. Hence, we provide a chart of different possible scenarios to summarise the GDPR's territorial scope at a glance. This should assist organisations, in particular, SMEs and other stakeholders such as DPAs to quickly assess whether and to what extent organisations are subject to the GDPR (See chart in Annex 1). CIPL recommends including this chart in the Final Guidelines.

CIPL further notes that the Article 29 Working Party previously published FAQ documents[4] to accompany its guidelines and recommends that the EDPB continue this practice for the present guidelines. CIPL also recommends including in such an FAQ the examples contained in the Draft Guidelines and ensuring that these are updated on a periodic basis. They should include the specific cases that are submitted to the EDPB. Finally, to ensure that the FAQ is easily accessible to all stakeholders on a need-to-know basis, CIPL recommends it be stored in a dedicated section of the EDPB website.

Finally, CIPL welcomes that the Draft Guidelines[5] mention the need for controllers and processors to assess how EU Member States' national laws, adopted on the basis of the GDPR, apply to them (in addition to determining whether and how Articles 3(1) and 3(2) of the GDPR apply). With more than fifty opening clauses providing Member States with the ability to adopt specific and varying national rules,[6] controllers and processors face an additional layer of complexity for their operations in the EU. Unfortunately, national laws do not apply consistent criteria for determining their own territorial scope, with most Member States' laws applying criteria equivalent to Article 3(1) GDPR,[7] while others, for instance France, applies criteria equivalent to Article 3(2) GDPR.[8] This may result in several laws applying to the same situation or even conflicts of laws within the EU itself.

While CIPL understands that scrutinising national laws is outside the scope of the EDPB's remit, CIPL stresses that this lack of consistency of criteria for national law jurisdiction within the EU produces unintended negative effects, potentially affecting the level of protection and legal certainty for individuals and adds another layer of legal complexity for controllers and processors. CIPL would ask the EDPB to consider this when drafting the Final Guidelines and to bring the practical consequences of these diverging legislative approaches of the Member States to the attention of the European Commission.

---

[3] See Decision of the EEA Joint Committee, No. 154/2018 of 6 July 2018, which states in Article 1(b) that EEA countries are considered "Member States" for purposes of the GDPR, available at http://www.efta.int/media/documents/legal-texts/eea/other-legal-documents/adopted-joint-committee-decisions/2018%20-%20English/154-2018.pdf.

[4] See, for example, WP29 Guidelines on Data Protection Officers as last revised and adopted on 5 April 2017, available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44100, at pages 20-25 (Annex - DPO Guidelines: What you Need to Know).

[5] *Supra* note 1 at page 12.

[6] For example, Article 8 on Children's Age of Digital Consent, Article 35(4) permitting data protection authorities to define their own list of high risk processing operations warranting a DPIA and Article 37(4) permitting Member States to require the designation of a DPO in circumstances additional to the mandatory GDPR requirements.

[7] Examples include Belgium, The Netherlands and Ireland.

[8] See Article 3(2) of Ordinance No. 2018-1125 of 12 December 2018, available at https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=E8836CFEE032185D84E1C940F123A15A.tplgfr31s_2?cidTexte=JORFTEXT000037800506&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000037800456.

I. Application of the Establishment Criterion — Article 3(1)

a) Consideration 1: "An establishment in the Union" (page 4 of the Draft Guidelines)

CIPL welcomes the EDPB's recognition that the notion of "establishment" and therefore the application of the GDPR is not without limits. In this context, the EDPB confirms, in particular, that a non-EU entity should not be considered as having an establishment in the Union "merely because the undertaking's website is accessible in the Union".[9]

CIPL notes however that, in addition to **Example 1** which describes a situation where there is an establishment in the EU, other detailed examples are needed of situations where the establishment threshold would not be met.

The Draft Guidelines clarify the criteria that qualify the organisation as having an establishment in the EU. In addition to the criteria of "effective and real exercise of activities" and "a stable arrangement", they provide that the mere presence in the EU of one single employee or agent of the non-EU entity may be sufficient to trigger the application of the GDPR. The Final Guidelines should explicitly state, however, that the activities of such an employee or agent of a controller should be directly related to the processing of personal data. Companies often offer multiple and diverse business lines of products and services within the same company, establishment, or legal entity. These do not necessarily trigger the processing of personal data, especially where the client of the company is not an individual, but another company. As specified in Recital 14, the GDPR does not cover the processing of personal data of legal entities. Therefore, the Final Guidelines should further clarify that having one single employee could constitute a stable arrangement, but the GDPR is only applicable if the acts of such an employee are directly related to personal data processing by the controller (which is consideration 2).

Finally, the Draft Guidelines assert that where the processing of personal data falls within the territorial scope of the GDPR, all provisions of the Regulation apply to such processing. The Draft Guidelines do not specify that the GDPR obligations only apply to the specific processing activity itself that triggers the application of the GDPR and not automatically to all the other processing activities of the legal entity established in the EU. It is important that the EDPB further clarify this so that organisations are able to define the precise scope of their obligations. For example, the entity might be obliged under the GDPR to appoint a DPO. However, that DPO's tasks should be limited to personal data processing to which the GDPR applies (i.e. to the services that trigger the extraterritorial scope of the GDPR). CIPL recommends, therefore, that the EDPB confirm this position.

[9] *Supra* note 1 at page 5.

Summary of CIPL Recommendations:

- Provide more detailed examples of where the establishment threshold would not be met.

- Clarify that having one single employee constitutes a stable arrangement only if the acts of such an employee are directly related to personal data processing.

- Confirm that GDPR obligations only apply to data processing that is subject to the GDPR.

b) Consideration 2: Processing of personal data carried out "in the context of the activities of" an establishment (page 6 of the Draft Guidelines)

CIPL welcomes the recognition by the EDPB that the interpretation of "processing in the context of the activities of an establishment of a controller or processor" must find a balance between a too narrow and too broad understanding. CIPL welcomes, in particular, the acknowledgement that mere presence in the EU does not trigger the application of the GDPR in the absence of a further nexus (subject to the clarifications requested in these comments, under point a) above).

In addition, CIPL welcomes that the Draft Guidelines propose an *in concreto* analysis when assessing whether the processing of personal data is carried out in the context of the activities of an establishment in the EU. CIPL agrees that each case should be analysed on a case-by-case and contextual basis, especially in light of the growing sophistication and complexity of organisations and business models. As the EDPB rightly states, this ensures that situations in which the link between the establishment and the data processing activities is too remote do not fall under the GDPR.

More generally, CIPL wishes to highlight that the reference to the processor (as opposed to only the controller) for triggering the territorial scope of EU data protection legislation is new in the GDPR. The Draft Guidelines often refer to the controller and not the processor.[10] It is therefore questionable to what extent the case law, arising from Directive 95/46/EC, on the meaning of processing "in the context of the activities of an establishment" can be applied to the activities of a processor. In view of this case law and the nature of the role of a processor, it would be appropriate to rely on a stronger and narrower nexus for processors.

The EDPB does support this point of view later on in its Draft Guidelines, when it states that considering the existing case law, "the effect of processing being carried out in the context of the activities of an EU establishment of a processor is less clear"[11] and hence should be considered separately from the controller. CIPL wishes to underline that the processor processes data only on instructions from the controller, as specified by the contract with the controller. As such, processing services by a processor are never carried out in the context of the activities of its own establishment in the EU.

i) Relationship between a data controller or processor outside the Union and a local establishment in the Union

CIPL suggests that the EDPB take a more flexible approach to the criteria used to assess whether the processing of personal data is carried out in the context of the activities of an establishment

[10] *Id*. at page 5, for instance, notes that "[t]he threshold for 'stable arrangement' can actually be quite low when the centre of activities of a controller concerns the provision of services online" (emphasis added).
[11] *Id*. at page 10.

of a controller or processor in the EU. The EDPB highlights the criterion of an inextricable link between the activities of the EU establishment and the data processing activities. If there is an inextricable link between the data processing and the EU establishment, the data are processed in the context of this establishment. This is also the consequence of the case law of the CJEU, in particular the Google Spain ruling.[12]

However, as rightly recognised by the EDPB, it is not always evident when an inextricable link exists. The notion of an "inextricable link" is subjective, contextual and variable in practice. CIPL recommends that the EDPB explain that there only be a presumption that EU law may apply because of an "inextricable link" and that a controller or processor could rebut it on the basis of the specific processing, activities and facts at issue. In this context, CIPL welcomes the use of the expression "may be indicative of processing by a non-EU controller or processor being carried out in the context of the activities of the EU establishment"[13] in the paragraph relating to revenue raising in the Union and recommends that the same wording be used throughout the whole section.

Similarly, in **Example 2**, the EDPB asserts that the activities of an establishment in the Union and the data processing activities of a controller or processor established outside the EU may be inextricably linked, triggering the applicability of EU law. The EDPB should clarify which elements of a controller's or processor's data processing comes within the scope of the GDPR. As currently worded, **Example 2** could be understood to mean that in such a scenario, all processing of personal data by the non-EU establishment becomes subject to the GDPR. That would be excessive and it should be clarified that the case-by-case analysis should not stop with finding the link, but should also examine which particular processing falls within the scope of the GDPR as carried out in the context of the EU establishment (and which particular processing does not fall within the scope of the GDPR).

ii) Revenue raising in the Union

In addition, the Draft Guidelines provide that revenue-raising activities by an EU establishment that can be "inextricably linked" to the processing of personal data taking place outside of the EU aimed at individuals in the EU may be indicative of activities being carried out "in the context of the activities of the EU establishment".

In relation to **Example 2,** CIPL would welcome confirmation from the EDPB that for the GDPR to be applicable, the activities of the EU office must be designed and specifically targeted at boosting the website sales (as opposed to having the simple effect of boosting the website sales). In other words, the GDPR should only apply in situations where the EU entity plays a significant and active role in the revenue raising.

In addition, under the Draft Guidelines, it would appear that a financial interest of an EU parent company (e.g. a conglomerate) in its non-EU investments that rely on processing of personal data as part of their business model would be sufficient to trigger the applicability of the GDPR. The Draft Guidelines' focus on financial interest as a nexus to the activities of uniquely non-EU companies processing personal data of non-EU data subjects seems to suggest that mere establishment of an EU shell company, holding company, or indeed the setup of a conglomerate

[12] Case C-131/12, Google Spain and Google, available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=148236.
[13] *Supra* note 1 at page 7.

parent company will *de facto* mean that all holdings of such companies might be subject to the GDPR worldwide. CIPL suggest that the Final Guidelines clarify that a mere financial interest (e.g. tax structure, exchange listing) without a more operational role in the activities of the non-EU processing is insufficient to bind non-EU affiliates of an EU-parent company to the GDPR.

CIPL would recommend adding specific examples to further illustrate this case:

Example 2(B) — A delivery app company based in Chile has its parent company in Luxembourg. The corporate and strategic decisions relating to the Chilean company are taken in Luxembourg (e.g. the board meetings are held there), but the Luxembourgish parent company does not exercise any operating activity or decision-making with respect to the personal data processed in Chile. In this case, the mere shareholding interest in the activities of the non-EU processing is insufficient to bind the Chilean affiliates to the provisions of the GDPR.

Example 2(C) — An EU-based investment company takes ownership interest in numerous non-EU companies processing personal data of non-EU users collected exclusively outside of the EU. These companies become the subsidiaries of the parent within a corporate group. While the parent company has a financial interest in the success of the subsidiaries, it exercises no operational control over them. The nexus to personal data processing is insufficient to bind the non-EU affiliates under the GDPR.

Summary of CIPL Recommendations:

- Apply a rebuttable presumption to the qualification of an "inextricable link" between the data processing and the EU establishment.

- Clarify that the activities of the EU establishment have to be designed and targeted at raising revenue in the EU (Example 2).

- Clarify that a mere financial interest without a more operational role in the activities of the non-EU processing is insufficient to bind non-EU affiliates of an EU-parent company to the GDPR and add relevant examples to illustrate this point in concrete terms.

c) Consideration 3: Application of the GDPR to the establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not (page 8 of the Draft Guidelines)

Article 3(1) is clear that the GDPR may also apply to processing of personal data that is not performed in the EU ("regardless of whether the processing takes place in the Union or not") and CIPL agrees with the corresponding EDPB comments as well as with **Example 5** on page 8 of the Draft Guidelines. CIPL underlines however that **Example 5** refers to the case of a Singaporean branch that is not a legally distinct entity from the EU headquarters which determines the purpose and means for the processing in Singapore. In the case of an EU holding company which has non-EU affiliates that are controllers in their respective territories outside the EU, the GDPR should not apply to the processing activities of its affiliates. The term "in the context of" should not be broadly extended to cover the activities of non-EU controllers belonging to EU holding companies (see above comment in Section I. b) ii)).

With regards to the location of the data subjects for the purpose of the application of Article

3(1), CIPL suggest a narrow and reasonable interpretation that helps minimise practical implementation difficulties for companies. In this context, CIPL would like to highlight the practical consequences of **Example 4** of the Draft Guidelines. National laws of third countries have their own specific criteria to define their territorial scope and may contain provisions similar to Article 3(2)(a) of the GDPR whereby they are applicable in cases where companies located outside of their territory are offering goods or services or monitoring the behaviour of data subjects within their borders.[14]

In particular, when there is a possibility that the GDPR would apply in addition to local laws that have been recognised as adequate under Article 45 of the GDPR as per EU standards, a "rule of reason" should enable organisations to apply either local law or the GDPR. This solution would not reduce the protection afforded to individuals if the local law has been assessed as being "essentially equivalent" to EU standards. The application of this "rule of reason" would need to be assessed on a case-by-case basis. CIPL also recognises that there are cases where public interest mandates for the application of the GDPR to extend its protections to the benefit of individuals.

In **Example 4**, the core of the processing activity — and in particular the collection of personal data from data subjects — for the use of the car-sharing application happens in Morocco, Algeria and Tunisia. CIPL recommends further investigating practical solutions, in line with the approach taken by the CJEU in the Weltimmo case[15] where it accepted the application of a national law of the country where the activities, in essence, took place (in a case where it had to decide between two applicable Member State laws).

In addition, CIPL wishes to mention as a possible reference and starting point to building solutions, the opinion of Advocate General Szpunar in Google Inc.v CNIL. He clearly explains the potential complexities and challenges when several laws may apply to the same situation or when laws are given broad extraterritorial effect: "If an authority within the Union could order dereferencing on a global scale, a fatal signal would be sent to third countries, which could also order dereferencing under their own laws. Let us imagine that for some reason third countries are interpreting some of their rights so as to prevent people in a Member State of the Union from accessing information sought. There would be a real risk of levelling down, at the expense of freedom of expression, on a European and global scale".[16]

Summary of CIPL Recommendations:

- Recognise the practical difficulties of several laws applying cumulatively, including national laws that have been deemed adequate from an EU perspective.

- Further investigate practical solutions to such difficulties in light of the CJEU case law.

[14] See, for example, Article 3(II) of the Brazilian Data Protection Law (Lei Geral de Proteção de Dados Pessoais), available at http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.
[15] See Case C-230/14, Weltimmo, available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=168944&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=164239.
[16] See Opinion of Advocate General Szpunar, Case C-507/17, Google Inc. v CNIL, ECLI:EU:C:2019:15, at para. 61, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CC0507.

d) Application of the establishment criterion to the controller and processor (page 9 of the Draft Guidelines)

CIPL welcomes the clarification from the EDPB that the existence of a relationship between a controller and processor does not automatically trigger the application of the GDPR to both, should one of them be subject to the GDPR as per Article 3(1) and that each entity needs to meet the applicability test separately.

In particular, if a non-EU controller chooses a processor in the Union, the non-EU controller will not automatically become subject to the GDPR as a result of this choice. In other words, simply instructing an EU processor does not mean that the non-EU controller is carrying out processing "in the context of the activities of the processor". The non-EU controller is processing data in the context of its own activities and the processor is merely providing a processing service which is not "inextricably linked" to the activities of the controller. The same reasoning would apply in case a non-EU processor chooses a sub-processor in the Union.

According to the Draft Guidelines, a processor will not be considered an establishment of a controller "merely by virtue of its status as processor" and that "unless other factors are at play" the processor's establishment will not be an establishment of a controller.[17] CIPL suggests that the EDPB clarify that the same reasoning should apply to a non-EU processor using an EU sub-processor. As it is unclear what these "other factors" could be, CIPL recommends that the EDPB clarify these criteria by specifying some precise examples.

i) Processing by a controller in the EU using a processor not subject to the GDPR

The EDPB states that a controller may need to consider imposing, by contract, the obligations placed by the GDPR on processors who are not otherwise subject to the GDPR. This broad statement goes beyond the requirements of Article 28(3) of the GDPR and may cause unreasonable demands from EU controllers on their non-EU processor (e.g. by demanding that the processor will comply with all processor obligations under the GDPR). CIPL recommends the deletion of this argument or at least a clarification that a contract compliant with Article 28(3) is sufficient, since it indirectly covers Articles 12 to 23 and 33 to 36 of the GDPR. This same clarification should also be reflected in **Example 6**.

ii) Processing in the context of the activities of an establishment of a processor in the Union

CIPL also welcomes the much awaited clarification[18] that confirms the common interpretation that processors are subject only to their "GDPR processor obligations" when they act on the instructions of a non-EU data controller.

The EDPB recognises that the effect of processing being carried out in the context of the activities of an EU processor is not clear. As the situation where an EU processor is acting on the instructions of a non-EU controller is not addressed in the GDPR and because the GDPR provisions are not really adapted to this specific scenario, the Draft Guidelines dig into the details of Article 28 of the GDPR to define how this provision applies to this specific situation. CIPL welcomes the exercise performed by the EDPB because it attempts to bring clarity on the interpretation of the law. While there may be instances where non-EU controllers select EU

[17] *Supra* note 1 at pages 9 and 10.
[18] This was an existing and open question under Directive 95/46/EC which had not been clarified.

processors because they are subject to the GDPR, the EDPB should also bear in mind the specificity of this situation and be pragmatic in its approach to avoid making EU processors "unattractive" for markets outside of the EU. We highlight the following practical issues of imposing too many specific obligations on the EU processor providing services to a non-EU controller:

a) As part of the GDPR processor obligations, the EDPB considers that "the processor shall maintain a record of all categories of processing carried out on behalf of the controller, as per Article 30(2)". While CIPL agrees this statement is in line with the GDPR, CIPL wishes to further highlight the practical complexity of such a requirement in this case and the fact that the GDPR may have not been drafted originally to address it. In this specific situation, it is worth mentioning that the "controller" is not within the scope of the GDPR[19] and is therefore not a "controller" in the sense of Article 30(2) of the GDPR. It may, therefore, be very challenging from a practical perspective for the processor to be able to collaborate with the controller to obtain the information necessary to maintain its own record of processing as the controller itself is not subject to the obligation to maintain a record of processing. The situation is different when the controller is subject to the GDPR as it is under the obligation to maintain a record as per Article 30(1) and knows that the processor has a similar obligation as per Article 30(2). When the processor acts on the instructions of a non-EU controller, who is not bound by the GDPR, such a processor would run a higher risk of not being compliant with this provision. The requirement to maintain a record of processing is designed to enable processor accountability and data mapping and, ultimately, an efficient exercise of individual rights afforded by the GDPR. However, having a strict interpretation of the obligation for the processor to maintain a record may not be relevant in this specific case as the data subjects do not benefit from these rights in the first place.

b) CIPL believes that it would be unreasonable for the Article 28(3) requirement to "immediately inform the controller if...an instruction infringes this Regulation" to apply in a scenario where the controller is not subject to the GDPR. It is indeed to be expected that a controller which does not need to comply with the GDPR may potentially give instructions that do not comply with the GDPR. The EDPB should clarify that the processor is not subject to the obligation to "immediately inform the controller" because this provision relates to "the assistance to the data controller in complying with its (the controller's) own obligations under the GDPR".[20] However, in cases where the processor believes that the instructions given to it by the non-EU controller would cause it to infringe the GDPR, it will have to object to these instructions in order to avoid being in breach itself.

c) There are more situations where the EU processor must comply with the GDPR rules but needs the controller's cooperation to do so, yet the controller is not subject to the GDPR. In practice, it may be quite challenging for a processor (who is supposed to be acting on the instructions of a controller) to actually impose on the controller the obligation to enter into agreements specific to EU law, such as an Article 28(3) data processing agreement. In cases where the non-EU controller is not willing to sign an

[19] CIPL would like to highlight that such a concept may not even exist or be applicable under the law to which the non-EU entity is subject to.
[20] *Supra* note 1 at page 11 setting the list of obligations of the EU processor acting on the instructions of a non-EU controller.

Article 28(3) agreement (although the processor offered to enter such an agreement), the processor should not be responsible for this situation.

d) Article 28(2) of the GDPR requires the processor to obtain the written authorisation of the controller to engage another processor. As such authorisation may be challenging to obtain from a non-EU controller in practice, the EDPB should clarify that compliance with this provision shall not be deemed the sole responsibility of the processor. The processor can only be accountable under the GDPR (i.e. take measures to enable compliance and be able to demonstrate them) to the extent it does not require the active collaboration of another organisation that is not itself accountable under the GDPR. Therefore, CIPL would welcome clarification from the EDPB that the EU processor should only have to meet the GDPR requirements to the extent they are in its exclusive sphere and control.

e) While CIPL understands that the provisions of Article 46(1) of the GDPR would require Chapter V of the GDPR to apply in cases of international data transfers performed by the EU processors, it wishes to describe below the reality and practical consequences of such application: When non-EU personal data is sent back by the EU processor to the non-EU controller, this transfer is done on behalf and on the instructions of the non-EU controller and is not an independent decision from the EU processor. In this situation, the personal data that flows back to the non-EU controller was never collected from the EU. The transfer has the mere effect of restoring the former state before the initial transfer of data to the EU processor — i.e. a non-EU controller processing non-EU personal data. Moreover, applying a GDPR standard when data is flowing back to the controller would not add value to the protection of individuals who did not benefit from the protection of the GDPR by the non-EU controller in the first place. In other words, just as the EU processor was free to receive the personal data from the non-EU controller by means of an inbound international transfer with no associated GDPR related requirements, the processor may return the data through an outbound international transfer under that same standard.

f) The same reasoning would apply when the EU processor processing personal data from non-EU controller uses a non-EU sub processor in a different country than where the non-EU controller is located. Although this transfer would not restore the former status for the data subjects (because the level of protection in the other third country might be different than that of the non-EU controller), it would add no value to subject this transfer to a GDPR standard — i.e. to allegedly protect individuals who did not benefit from the protection of the GDPR by the non-EU controller in the first place.

g) For both situations — non-EU personal data flowing to a non-EU controller or non-EU sub-processor — it appears that Chapter V of the GDPR was not drafted to address such scenarios. Under Article 46(1) of the GDPR, international transfers can only happen "on condition that enforceable data subject rights and effective legal remedies for data subjects are available", but these rights and remedies were never afforded to the non-EU data subjects in the first place. Applying Chapter V to these situations would not add any value to the protection of individual rights while putting unreasonable administrative burdens on EU processors. In light of this, CIPL requests the EDPB and the EU Commission, in consultation with industry and relevant stakeholders work further towards identifying concrete and pragmatic solutions for EU processors.

If, on the other hand, the EDPB were to decide that EU processors acting on the instructions of non-EU controllers should comply with the GDPR provisions on international transfers of data, more guidance would be needed on the way to comply with this in practice. When the non-EU controller is not in an adequate country, the parties will have to resort to standard data protection clauses as per Articles 46(2)(c) or (d) or 46(3) of the GDPR. The current clauses approved by the EU Commission (that cannot be modified by the parties) do not cover the specific situation of a processor to controller relationship (P to C) where the processor is the data exporter from the EU and the controller is the data importer from the EU.[21]

Finally, CIPL agrees with the EDPB that controllers and processors should not seek to circumvent applicable laws and use the Union territory as a "data haven". However, in light of some of the unintended practical consequences stemming from the application of the GDPR in situations where data subjects do not benefit from the protection of the GDPR in the first place, CIPL recommends that a pragmatic approach be taken and that the interpretation of the GDPR be balanced with other rights and freedoms, such as the freedom to contract and to conduct business of controllers and processors.

In summary, CIPL recommends that the Final Guidelines adjust the obligations of the EU processor when it acts on the instructions of a non-EU controller that is not subject to the GDPR in order to frame the "GDPR processor obligations" more pragmatically and to take into account the commercial and factual reality.

Summary of CIPL Recommendations:

- Provide examples of factors that are relevant to consider when a processor may be considered as an establishment of a controller.

- Clarify that for relations between an EU controller and a non-EU processor, a contract compliant with Article 28(3) is sufficient and amend Example 6 accordingly.

- For relations between a non-EU controller and an EU processor, adjust the "GDPR processor obligations" to take into account the commercial and factual reality and further investigate concrete solutions.

II. Application of the Targeting Criterion — Article 3(2)

As a preliminary remark, CIPL highlights that although Article 3(2) applies to both controllers and processors, in practice it is likely that Article 3(2) will only be relevant to controllers that are either offering goods or services to data subjects in the Union (Article 3(2)(a)) or controllers that are monitoring data subject behaviour taking place in the EU (Article 3(2)(b)). As a matter of fact, all of the examples provided by the EDPB under this section relate only to the application of Article 3(2) of the GDPR to controllers.

[21] Existing controller to processor clauses only cover situations where the controller is the data exporter and the processor is the data importer. The EU Commission has not produced standard data protection clauses dealing with the scenario of a data processor as the data exporter. In addition, such cases are not addressed by the Article 29 Working Party in its FAQ on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC. See FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC, adopted on 12 July 2010, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp176_en.pdf.

When a non-EU controller who is subject to the GDPR under Article 3(2) uses the services of a processor outside of the EU, it generally does so on the basis of an Article 28(3) GDPR data processing agreement. In other words, the processor is not independently subject to the GDPR, but has to comply with the instructions of a data controller subject to the GDPR as per Article 3(2) and by virtue of a contractual arrangement under Article 28(3). Even if following these instructions results in the processor providing goods or services to, or monitoring the behavior of, individuals in the EU, the processor is not independently subject to Article 3(2).

The Draft Guidelines explain this situation clearly when the controller is subject to the GDPR pursuant to Article 3(1) and uses a processor not subject to the GDPR.[22] To ensure consistency, the Final Guidelines should confirm that this is also the case when a controller is subject to the GDPR pursuant to Article 3(2) and uses a processor not otherwise subject to the GDPR under Article 3(1). Additional considerations on this topic are also included in points a) and b) below.

a) Consideration 1: Data subjects in the Union (page 13 of the Draft Guidelines)

CIPL welcomes the clarification that Article 3(2) requires a proactive targeting or offering of goods or services from a controller or processor. The mere processing of personal data of individuals in the EU alone, absent an establishment of the controller or processor does not automatically trigger the application of the GDPR.

CIPL believes, however, that **Example 9** may be a misleading illustration of Article 3(2). In this example, the EDPB suggests that for the data processing not to be within the scope of the GDPR, all three factors (US citizen, in Europe only on holiday, app exclusively directed at US market) need to be present. On the contrary, it should be emphasised that the mere fact of a company being based in the US and exclusively targeting US subjects in the US is sufficient to be outside the scope of the GDPR. The fact that the US customers, who use US originated products and services, are temporarily or even for a longer period of time in the EU should not trigger the application of the GDPR for that app. This should be the case even if there is a further offering of services or monitoring of their behaviour while they are in the EU and even if the company knows they are temporarily in the EU. This is a fairly common scenario as consumers and employees are highly mobile and the EDPB should explicitly clarify that these situations do not trigger GDPR application.

According to the EDPB, "Processing activities which are 'related' to the activity which triggered application of Article 3(2) also fall within the territorial scope of the GDPR. The EDPB considers that there needs to be a connection between the processing activity and the offering of good or service, but both direct and indirect connections are relevant and to be taken into account".[23] Due to the wide variety of business and commercial offers, including cases where no payment is required from the data subject and the potential processing activity stemming therefrom, CIPL would welcome clarification from the EDPB on the notion of "indirect connections" to further specify and illustrate this situation. CIPL suggests the EDPB confirm that the processing activity should be clearly linked to the initial activity (which triggered the application of Article 3(2)) to be considered subject to the GDPR.

[22] *Supra* note 1 at page 9 "i) Processing by a controller in the EU using a processor not subject to the GDPR".
[23] *Id*. at page 15.

The Draft Guidelines[24] contain a list of factors that could be taken into account in considering whether goods or services are offered to data subjects in the Union. CIPL would welcome more clarification on the following criteria: "The international nature of the activity at issue, such as certain tourist activities".[25] Not all tourist activities are directed internationally nor automatically constitute the offering goods or services to data subjects in the EU, just because an EU individual may use the service or access a website for a tourist attraction. CIPL suggests that the Final Guidelines confirm that just because a particular destination is known to be a popular tourist attraction for residents around the world, including residents in the EU, it should not, on its own, be determinative in making the company subject to the GDPR.

Summary of CIPL Recommendations:

- Confirm that a processor offering goods or services or monitoring individuals on the instructions of a controller subject to the GDPR as per Article 3(2) is not independently subject to Article 3(2) GDPR.

- Further elaborate in Example 9 facts that are sufficient for the specific situation to be outside the scope of the GDPR.

- Provide further explanations and examples of "indirect connections" between processing activities and the offering of goods and services.

- Clarify the notion of an international activity and confirm that a particular destination known to be a popular tourist attraction should not be determinative for Article 3(2) purposes.

b) Consideration 2a: Offering of goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the Union (page 14 of the Draft Guidelines)

The EDPB considers that processing activities that are directly and indirectly related to the offering of goods and services would also fall under the scope of the GDPR. CIPL recommends including concrete examples to illustrate this, particularly in cases of processing activities that are indirectly related to the offering of goods and services. The relevance of this extension is questionable, in particular, in cases of ancillary processing activities relating to the maintenance of network security or fraud detection and prevention.

CIPL would like to submit the following practical case to the EDPB:

An Australian professional services organisation contracts with an Australian national to assist with the preparation of his/her Australian tax return. The individual has been relocated by his company to Denmark. The activities of the Australian professional services organisation are not specifically directed at the EU market. Similar to the US direct app in **Example 9**, CIPL does not believe that this Australian organisation would be considered to be providing services to data subjects in the Union and therefore subject to Article 3(2)(a) of the GDPR. This interpretation should not change even if multiple individuals are relocated to the EU.

In addition, CIPL suggests the EDPB perform a more in depth analysis of how the GDPR would apply to a non-EU processor under Article 3(2)(a). In a typical scenario, the processor makes an "offer" to the controller to process the personal data of data subjects on its behalf. Considering

[24] *Id*. at pages 15-16.
[25] *Id*. at page 15.

that this offer of services is not addressed to the data subjects themselves, the processor has no intention of targeting them directly in the sense of Recital 23 of the GDPR. Consequently, the "intentional targeting" criteria are not suitable for concluding a processor's intention under Article 3(2)(a), as the processor rarely has influence over the targeting itself.

CIPL supports the view taken in **Example 13** that human resources management, including salary payment, cannot be considered as an offer of service to the French and Italian employees by the company based in Monaco. CIPL would also like the EDPB to address the situation where the company based in Monaco outsources its payroll activities to a third party payroll processor outside of the EU. CIPL recommends the EDPB confirm that in this case, the external payroll company would not be subject to Article 3(2)(a) of the GDPR. Although the processing activities include employee data, the external payroll company offers B2B services and provides them to the Monaco company only and not to its employees individually. CIPL suggests the EDPB add this example, using the same facts, as follows:

Example 13(B) — The Monaco based company with French and Italian employees has outsourced its payroll activities to a payroll provider in Brazil. This payroll provider manages the salary payment process and provides pay slips to employees of the company in France and in Italy. The Brazilian payroll provider is acting on the basis of a service agreement entered into with its client, the company in Monaco. The Brazilian company has no contractual relationship with the individual employees. Although the Brazilian payroll provider is processing personal data of employees in France and Italy, it is providing services to the company in Monaco only. It is not providing services to data subjects in the Union. As a result, Article 3(2)(a) of the GDPR should not apply to the Brazilian payroll provider.

Summary of CIPL Recommendations:

- Confirm CIPL's interpretation with respect to the example of the Australian professional services organisation and the relocation of its customer to Denmark.

- Include Example 13(B) as outlined above in the Final Guidelines.

c) Consideration 2b: Monitoring of data subjects' behaviour (page 17 of the Draft Guidelines)

CIPL welcomes the fact that the EDPB considers that not all collection of personal data in the EU counts as monitoring, but that the purpose and intent of the controller or processor, in particular, to use the data for behavioural analysis or profiling must also be present to trigger GDPR application.

CIPL welcomes the clarification that monitoring should be understood as not only related to monitoring on the Internet, but also related to tracking though other types of network or technology involving personal data processing. The Draft Guidelines do not mention, however, any test or criteria for determining whether the GDPR applies in such cases. For example, how would organisations who engage in common, routine and essential activities in the security and employment contexts (e.g. email monitoring or device monitoring) be able to determine whether their specific activities constitute monitoring under Article 3(2)(b)? It would be helpful for the EDPB to provide more clarity around the application of Article 3(2)(b) to common tracking technologies involving personal data processing.

The EDPB also does not clarify whether the monitoring criterion applies only to the extent that

the processing activity involves the remote or online observation and analysis of individuals' behaviour in the EU over a certain period of time. This is important for services provided by consultancy firms or professional services firms. CIPL recommends the EDPB include the following example in its Final Guidelines:

A law firm in Chile is engaged by a company in Chile to assist with a corporate investigation of the company's subsidiary in Luxembourg. As part of this investigation, the law firm engages a Chilean forensic auditor firm to conduct eDiscovery services. The auditor — acting as a processor under the instruction of the Chilean law firm as controller — collects the laptops of board members of the subsidiary in Luxembourg, making forensic copies of certain files on these laptops for further investigation based on detailed instructions from the law firm. Given that the investigation is based on an image of the laptop which is made at a certain moment in time, such processing would not qualify as monitoring the behaviour of individuals who are in the EU by the Chilean forensic auditor.

In addition, the Final Guidelines should clarify when logging or tracking (such as counting subscribers' usage) becomes behavioural analysis and therefore "monitoring" subject to Article 3(2)(b).

The Draft Guidelines consider that online tracking through the use of cookies would be a monitoring activity for the purposes of Article 3(2)(b). It should be clarified, however, that tracking that is limited to aggregated analytical purposes with "no intention to target", such as analysing the frequency and use of different sections of a web page, although using cookie-based techniques, should not fall within the scope of the GDPR.

More generally, CIPL would welcome further clarification in the Final Guidelines as to whether network security monitoring falls under Article 3(2)(b). Organisations increasingly rely on network monitoring products and services to anticipate, prevent and respond to potential security and cybersecurity incidents or threats. Some of these tools, such as data loss prevention tools (DLP) appear to fall within the scope of the GDPR because they are intended for detecting incidents and security violations by identifiable people. Other tools, such as security information and event management (SIEM) tools or security operation center (SOC) services are aimed at ensuring network security as a whole by looking for unusual events or patterns that would suggest threats to the network. Such tools only monitor activities for network security purposes and do not monitor individuals as such. The Final Guidelines should confirm that network security activities are not to be considered as monitoring activities for the purposes of Article 3(2)(b) of the GDPR.

Finally, CIPL would welcome further guidance in the Final Guidelines on IP addresses. IP addresses are personal data and the monitoring of IP addresses assigned to individuals in the EU is a routine (and arguably global) activity of all present Internet companies worldwide, at a minimum for IP fraud or abuse detection (e.g. the monitoring of irregular traffic coming from EU IP addresses to detect DOS attacks and for other security-related purposes). The Draft Guidelines, in their present form, could be understood as rendering all monitoring of IP addresses subject to Article 3(2)(b) of the GDPR, in particular by reference to online tracking through the use of cookies or other tracking techniques such as fingerprinting.[26] However, this should not be the case as in some instances the monitoring of IP addresses is not intended to monitor individuals themselves but for other purposes as explained above. The EDPB itself

[26] *Id*. at page 18.

recognises that GDPR application is not without limits[27] and draws a clear distinction between unique, permanent and purposeful targeting of EU users versus incidental capture of EU personal data in the context of global targeting (See, in particular, **Example 14** about a Swiss university seeking to recruit German-speaking students that is not subject to the GDPR). This unintended application of the GDPR may also apply in relation to other technologies, such as MAC addresses and similar identifiers that are widely used without any intention to monitor individuals and their behaviour. The EDPB should provide guidance on these specific cases and confirm that the GDPR does not apply to these situations.

Summary of CIPL Recommendations:

- Clarify if monitoring also covers email monitoring in the employment context and more generally other common tracking technologies.

- Confirm that "monitoring" only covers online observation and analysis of individuals' behaviour over a certain period of time and not "instant" or "snapshot" activities and confirm CIPL's example outcome.

- Clarify when logging or tracking (such as counting subscribers' usage) becomes behavioural analysis and therefore "monitoring".

- Clarify that tracking, limited to aggregated analytical purposes with no intention to target does not constitute "monitoring".

- Confirm that network security activities are not considered monitoring or profiling activities subject to the GDPR.

- Clarify that the use of identifiers that are not uniquely seeking to monitor or evaluate EU users is an insufficient nexus to trigger the GDPR.

III. Processing in a Place where Member State Law Applies by Virtue of Public International Law

CIPL recommends that the Final Guidelines clarify that a transfer of personal data from a country within the EU to an EU country's embassy or consulate located in a non-EU country would not be seen as a transfer to a "third country".

IV. Representative of Controllers and Processors Not Established in the Union

As a general comment, CIPL underlines that the designation of Article 27 representatives is instrumental for GDPR compliance of companies that do not have an establishment in the EU, but are subject to the GDPR under Article 3(2). This should not be overlooked when further defining the conditions applicable to the designation of the representative, the exemptions to such designation and the obligations and liabilities of the representative.

CIPL also welcomes the upfront clarification from the EDPB that "the presence of the representative within the Union does not constitute an 'establishment' of the controller and processor by virtue of article 3(1)".[28]

[27] See discussion on page 3 above and *Supra* note 1 at page 5.
[28] *Supra* note 1 at page 20.

a) Designation of a representative (page 20 of the Draft Guidelines)

The EDPB considers that the function of a representative in the Union is not compatible with the role of an external DPO, in part due to risk of compromise of independence. CIPL believes, however, that in cases where the non-EU based company also falls under the obligation to appoint a DPO under the GDPR and chooses to appoint an external DPO, the same organisation should be able to propose both services to its clients, provided, of course, the appropriate governance and ethical walls are put in place internally to ensure due separation of functions and information. This would enable better communication and cooperation between the representative of the data controller or processor and the external DPO and better compliance overall. This would be even more relevant in cases of exercise of data subject rights. As stated by the EDPB itself, the representative must facilitate the communication between the data subject and the controller and processor in order to make sure such rights are effective. SMEs and smaller organisations would welcome this solution as well.

In addition, the Draft Guidelines contemplate that the representative would serve as a primary point of contact with the Supervisory Authority and would carry out certain tasks that — in principle — fall within the domain and are the duty of the DPO. As a matter of fact, Article 39(1)(d) of the GDPR provides that one of the tasks of the DPO is to cooperate with the Supervisory Authority. Therefore, CIPL recommends that the Final Guidelines make clear that Supervisory Authorities should engage directly with the DPO, not with the appointed representative in routine cases.

Summary of CIPL Recommendations:

- Reconsider the possible mutualisation of the Article 27 representative and DPO roles in cases where appropriate governance and ethical walls are put in place.

- Clarify that Supervisory Authorities should engage directly with the DPO, not with the appointed representative in routine cases.

c) Establishment in one of the Member States where the data subjects whose personal data are processed are (page 22 of the Draft Guidelines)

CIPL agrees that the appointment of the representative in the country where a significant number of data subjects are located is a good practice for non-EU companies subject to the GDPR. This should, however, always remain as a voluntary decision by the company in line with Article 27(3) of the GDPR.

The EDPB also confirms that in the absence of an establishment in the Union, a controller or processor cannot benefit from the one-stop-shop under Article 56 of the GDPR.[29] This means that non-EU companies subject to the GDPR by virtue of Article 3(2) cannot benefit from the one-stop-shop in cases where their activities in the EU extend to several Member States.

CIPL would like to mention, however, that the earlier WP29 guidelines on Personal data breach notification[30] provide that when a non-EU controller subject to the GDPR under Article 3(2)

[29] *Id*. at page 12.
[30] WP29 Guidelines on Personal data breach notification under Regulation 2016/679, As last Revised and Adopted on 6 February 2018, available at https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827 at page 18.

experiences a breach and needs to notify the relevant DPA under Article 33 of the GDPR, it should notify the breach to the DPA in the Member State where the controller's representative is established. CIPL recommends that the Final Guidelines make reference to this recommendation to give a complete picture of the role and duties of the Article 27 representative.

In addition, CIPL also believes that the DPAs should incentivise the appointment and functioning of representatives in the Union since such representatives will play a central role in enabling compliance with the GDPR of non-EU companies and their cooperation with DPAs. This could be done by setting up a specific department or team within the DPA to address the questions and needs of Article 27 representatives and of their clients subject to the GDPR. Doing so would help promote the appointment of representatives and provide better compliance with the GDPR for the benefit of data subjects. This would also facilitate upfront communication and cooperation with the DPA which would be even more relevant if the representative is based in the country where a significant number of data subjects are located.

Summary of CIPL Recommendations:

- Confirm that Article 27 representatives can notify data breaches to the DPA in the country where they are established only.

- Work with DPAs to further incentivise the appointment of Article 27 representatives.

d) Obligations and responsibilities of the representative (page 23 of the Draft Guidelines)

The EDPB states that the representative must be in a position to efficiently communicate with data subjects and be able to use the language or languages used by the DPAs and the data subjects concerned. This can be quite challenging in a cross-border context. Therefore, CIPL proposes that this be worded as a best practice rather than as a legal requirement. Moreover, the EDPB should expressly note that "effective communication" may include the use of translators and translation tools. Personal fluency in local languages, while helpful, is not required.

In order not to discourage organisations from taking up an Article 27 role, CIPL would like to ask for clarification on the interpretation of the last sentence of Recital 80 of the GDPR. This provides that the representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor. In light of the potentially high fines or liabilities in cases of private enforcement actions, a restrictive reading of this wording could deter organisations from taking a representative role that is necessary to facilitate more effective GDPR compliance. The Final Guidelines should clarify that such representatives shall make themselves available to answer questions and provide evidence. They may be subject to the investigative powers of the DPA under Article 58(1) of the GDPR, but are only subject to the corrective powers of the DPA under Article 58(2) in a limited number of situations. Such an interpretation of Recital 80 is vital because it is not within the representative's remit to end infringements of the GDPR.

Even then, CIPL questions whether such enforcement proceedings can include the imposition of administrative fines on the representative itself where the non-compliance stems from the acts of a separate legal entity. CIPL recalls that Article 83(4) of the GDPR limits the imposition of fines to controllers, processors, certification bodies and monitoring bodies. It does not include the

representatives of organisations not established in the EU. Article 27 of the GDPR is silent on this topic. Recital 80 of the GDPR only mentions that the "representative should be subject to enforcement proceedings" which does not include the imposition of fines.

An important factor to consider is that it may be potentially challenging and even impossible for the Article 27 representative to get appropriate insurance to cover a potential liability that is calculated on the basis of a controller's turnover that may by far exceed its own revenues. For these reasons, CIPL recommends that the last sentence of the final paragraph in this section of the Draft Guidelines (i.e. "This includes the possibility to impose administrative fines and penalties, and to hold representatives liable") be deleted as it is not applicable to the representative.

Summary of CIPL Recommendations:

- Amend the wording in which the EDPB recommends that the representative be able to use the language or languages used by the DPAs and the data subjects.

- Clarify that the representative shall only be subject to the powers of the DPA as provided for in the GDPR.

- Delete the wording related to the possible imposition of fines on the representative.

V. Lack of clarification on the relationship between Article 3(2) and Chapter V on transfers of personal data to third countries

In addition to commenting on the Draft Guidelines, CIPL regrets that the EDPB has not been able to clarify the relationship between Article 3(2) of the GDPR and Chapter V of the GDPR.

By virtue of Article 3(2) GDPR, some non-EU organisations will be directly subject to the GDPR and will most likely have to appoint an Article 27 representative. For the proper functioning of the GDPR legal regime, it is essential that this issue is considered and clarified by the EDPB and the EU Commission in consultation with experts and stakeholders. It is not clear whether this has been considered at all during the legislative debates on the GDPR and there is no evidence that the text of the GDPR contemplates what the interaction should be between Article 3 and Chapter V. Yet, as the jurisprudence and developments on data transfers mechanisms take course, this point will become critical. Even if the text of Chapter V calls for a narrow interpretation, the spirit of the GDPR and the ambition on territorial scope calls for a different interpretation, perhaps even that Chapter V of the GDPR should not apply where the GDPR applies on the basis of Article 3. CIPL wishes to underline that having organisations implement and accumulate different layers of compliance obligations may ultimately run counter to operational compliance and accountability.

In essence, an accumulation of the obligations under Article 3(2) of the GDPR and Chapter V of the GDPR would not make sense. An organisation acting within the scope of Article 3(2) is required to put in place all the measures and safeguards of the GDPR. There is no added value in requiring this organisation to additionally comply with the obligations of Articles 46, 47 and 49 of the GDPR, because the organisation is already bound by all obligations stemming from these latter provisions.

CIPL would welcome a further discussion of these points and would like to play an active role in this dialogue, in collaboration with the EDPB and other relevant stakeholders.

- Organisations processing personal data directly from the EU

There are instances where organisations not established in the EU offer goods or services or monitor behaviour in the EU directly, without resorting to legal entities established in the EU. In such cases, the personal data flows directly from the data subject in the EU to the controller outside of the EU. The data subject normally does not qualify as a data controller or processor.

In this situation, the non-EU organisation is subject to all GDPR provisions by virtue of Article 3(2), including Article 13(1)(a) of the GDPR requiring that information be provided where personal data are collected from the data subject as well as the obligation to appoint an Article 27 representative and to provide the data subject whose personal data is being collected with the identity and contact details of the controller's representative. As a result, these organisations should not be subject to the provisions of Chapter V of the GDPR for the transfer of personal data between the EU data subject and the non-EU controller. CIPL underlines that this relationship as such does not qualify as a transfer of personal data between two legal entities. The Draft Guidelines also clarify that such a transfer cannot be made possible by the appointment of an Article 27 representative because it provides that such a representative within the Union does not constitute an establishment of a controller or processor by virtue of Article 3(1).[31]

This analysis is supported by Article 46 of the GDPR which provides that "[i]n the absence of a decision pursuant to Article 45(3), a controller or a processor may transfer personal data to a third country […]" (emphasis added). In the absence of a controller or processor in the EU, there can be no transfer of personal data under Chapter V. The controller, even though not established in the EU, collects personal data in the same manner as any other controller established in the EU, by the mere application of Article 3(2) of the GDPR without the need for additional safeguards that in any case already apply to it.

- Organisations processing personal data indirectly from the EU

In this situation, the processing of personal data is performed by an entity established in the EU that transfers data to a non-EU data processor for further processing. In such cases, the EU exporter and the non-EU importer should put in place appropriate safeguards as per Chapter V of the GDPR to cover the international transfer (in addition to signing an Article 28(3) agreement).

Where the transfer is made for the purpose of performing activities that would normally trigger the application of Article 3(2), such as activities related to the offering of goods and services or to the monitoring of individuals in the EU, CIPL recommends that the EDPB clarify that such a non-EU processor is not subject to Article 3(2) of the GDPR and shall not, in particular, have the obligation to appoint an Article 27 representative.

[31] *Supra* note 1 at page 20.

- Organisations proactively applying the GDPR

In case an organisation receives personal data from an EU established entity and decides to proactively apply the GDPR standards, it should be able to leverage these efforts and be free from the obligation to comply with the provisions of Chapter V of the GDPR (in addition to signing an Article 28(3) agreement).

Summary of CIPL Recommendations:

- Clarify the relationship between Article 3 and Chapter V of the GDPR.

- Provide that in situations where a non-EU organisation is subject to the GDPR by virtue of Article 3(2), it is not subject to the provisions of Chapter V of the GDPR.

- Clarify that non-EU processors acting on the instructions of a controller to offer goods or services or monitor behaviour in the EU are not subject to Article 3(2) of the GDPR.

Conclusion

CIPL is grateful for the opportunity to provide comments on key interpretation questions of the territorial scope of the GDPR under Article 3. We look forward to providing further input as the Guidelines are finalised.

If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com, Markus Heyder, mheyder@huntonAK.com, Nathalie Laneret, nlaneret@huntonAK.com or Sam Grogan, sgrogan@huntonAK.com.

ANNEX

Centre for Information Policy Leadership
Hunton Andrews Kurth

18 January 2019

GDPR Territorial Scope at a Glance