City of London Law Society Data Law Committee
Submission to the European Data Protection Board on guidelines 3/2018

The City of London Law Society ("CLLS") represents approximately 17,000 City lawyers through individual and corporate membership including some of the largest international law firms in the world. These law firms advise a variety of clients from multinational companies and financial institutions to Government departments, often in relation to complex, multijurisdictional legal issues. The CLLS responds to a variety of consultations on issues of importance to its members through its' 19 specialist committees.

This letter has been prepared by the CLLS Data law Committee (the "Committee").

We welcome the opportunity to respond to the European Data Protection Board's (EDPB's) public consultation on guidelines 3/2018 on the territorial scope of the GDPR (Article 3) ("Guidelines"). This submission is not confidential and we have no objection to it being published on the EDPB's website.

Unless otherwise stated, references to Articles, Recitals and Chapters are to articles, recitals and chapters in the GDPR and references to paragraphs are to paragraphs in the Guidelines.

1. Application of the establishment criterion – Article 3(1)

1.1 Processing of personal data carried out "in the context of the activities of" an establishment (paragraph 1(b))

Shared services

(A) It would be useful to have guidance on where Article 3(1) applies when multinational groups of companies set up shared services processing outside the EU. In particular, we would welcome further clarification on what amounts to an "inextricable link" between the activities of EU based establishments and the processing carried out by non-EU controllers in this context.

(B) For example, where a US head office HR team carries out benchmarking of performance scores and remuneration awards across global employees, it will necessarily need to access and process certain data of staff of EU based affiliates. These affiliates will meet the threshold as an establishment of the US parent company, but would this data flow be sufficient to meet the test of "processing in the context of the activities of [that establishment]" to bring the US parent company within the scope of the GDPR?

(C) In this scenario, data subject rights can be assured by a combination of the EU based affiliate being subject to the GDPR in full, and transfers from the EU affiliate to the US parent being subject to Chapter V, so there seems no policy reason for the US parent being made subject to the GDPR.

(D) Further clarification on these common intra-group transfers would be helpful, perhaps by way of additional examples.

Processor supply chains

(E) We would welcome further guidance on what "processing in the context of an establishment in the union" means with respect to processors and how this is understood to apply to their supply chains.

(F) In particular, it would be useful to have an example that demonstrates at which point in an EU processor's supply chain the processing is no longer being carried out "in the context" of the processing of that EU processor.

1.2 Processing in the context of the activities of an establishment of a processor in the Union (paragraph 1(d)(ii))

Requirements under Article 28(3)

(A) The guidance states that EU processors undertaking processing activities need to include the Article 28(3) requirements in their agreements with non-EU controllers even if the controller is not subject to the GDPR.

(B) However, the provisions of Article 28(3) have been drafted in the context of a controller who is subject to the GDPR. Whilst we appreciate the clarification that the processor is not subject to the requirements to assist the controller with its own obligations under the GDPR (and we therefore assume this need not be referred to in the processing agreement), it can still be challenging for an EU processor to persuade a non-EU controller, to whom the GDPR does not apply, to accept the inclusion of these terms.

(C) We would welcome guidance from the EDPB on how these provisions should be dealt with in practice in this context.

(D) In addition, it would be helpful if the EDPB were able to provide reassurance on the approach that the national supervisory authorities would take to enforcement action if all the Article 28(3) requirements were not met in these circumstances. For instance, would the national supervisory authorities take into account the EU processor's endeavours to persuade the controller to agree to the provisions of Article 28(3) even if they were not ultimately satisfied?

Breadth of obligation to inform controller of infringing instructions

(E) We would welcome clarification on the EDPB's statement on page 12 of the guidelines that quotes the GDPR as saying "*the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions*".

(F) This wording is taken from the end of Article 28(3) and the full text of that sentence is as follows (with the highlighting added) *"with regard to point (h) of*

the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions."

(G) It has previously been clarified that the reference to the first subparagraph should be to the third subparagraph ie Article 28(3). This therefore refers to the provision requiring the processor to make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28(3) and to allow for and contribute to audits.

(H) The statement in the Guidelines set out above in the context it is given suggests that the EDPB is interpreting this requirement to be broader than applying to the processor's obligation under Article 28(3)(h). It would be helpful if the EDPB could clarify its view on this.

Ethical issues

(I) The Guidelines state on page 12 that "*Union territory cannot be used as a "data haven", for instance when a processing activity entails inadmissible ethical issues*". Further guidance on the types of processing the EDPB is concerned about would be of assistance.

International transfers

(J) Processors subject to Article 3(1) have particular difficulties under Chapter V on which guidance would be useful. We appreciate that you may be planning to cover these issues in separate guidance on international transfers but we raise these concerns here for completeness given they are interlinked with the application of Article 3.

(K) In addition to the long running challenge of there being no processor to processor standard contractual clauses, there is now the challenge of there being no processor to controller clauses.

(L) Where there is an EU processor which needs to transfer personal data to its non-EU controller, there is, absent the non-EU controller being in an adequate jurisdiction, therefore no easy way to legitimise the transfer.

(M) In theory bespoke clauses approved by the relevant national supervisory authority could be a solution. However, we know, for instance, that both the UK and Dutch authorities are not currently prepared to approve bespoke clauses pending guidance from the EDPB. In any event, if approval would only be forthcoming if the clauses obliged the non EU controller to submit to audits by the processor, this is unlikely to be commercially acceptable. After all, from a non-EU controller's perspective, it is their data and they are not subject to the GDPR. It is hard to conceive why they would therefore agree to be audited by their processor.

(N) Non-EU controllers find this challenge difficult to understand given that in many cases they directly provided the personal data to the EU processor and then cannot receive it back. This risks putting EU processors at a disadvantage to their non-EU competitors.

2. Application of the targeting criterion – Article 3(2)

2.1 Consideration 1: Data subjects in the Union (paragraph 2(a))

Offers to corporate entities

(A) The GDPR refers to the offering to data subjects. The question frequently arises whether this includes where an offer is made by a non EU entity (with no EU establishment) to a corporate which, by its nature, acts through an individual. Whilst the communication is therefore with a data subject in the EU, the offer of goods or services is made to the corporate. Our view is that this does not fall within Article 3(2)(a) and clarification from the EDPB on this would be helpful.

(B) There are variations to the above example where the data subjects are the ultimate recipient of the service in their personal capacity. For example, in the area of employee advisory services the non-EU entity's offer is addressed to the EU corporate entity, and the contract would often be with the corporate entity since they would be paying for the services. However, the services would be provided directly to those employees who wish to avail themselves of the service.

(C) Another example is corporate health insurance. The insurer would target the corporate entity with a view to the employees being the end recipients of the service. Typically, there would be contract with the corporate, but there would be a separate insurance contract with each employee who wished to benefit from the insurance.

(D) This question also arises in an intra-group situation. For instance, you may have a subsidiary (company A) outside the EU which provides payroll services to another member of the group established in the EU (company B) in respect of its EU employees. The processing would be in the context of the establishment of company B but, as the Guidelines clarify, this does not make the processor subject to the GDPR directly in of itself. Company A would, however, be providing a service to a corporate and liaising with data subjects in the EU at the company B to do so. In addition, the service would benefit the employees of company B.

(E) Clarification on what amounts to an offer "to data subjects" for the purposes of Article 3(2)(a) would therefore be helpful.

Offers to own employees

(F) We would also welcome guidance on the scope of Article 3(2)(a) in terms of whether it applies to offers from non-EU companies to their employees within the EU.

(G) For instance, this could be where a US parent company offers a discount on the company's products to its EU based employees as an employee benefit, or where it provides other employee benefits such as a concierge service, health cover etc. Typically these benefits would be provided by third parties under a contract with the employing entity. Can it be said that the parent company is offering goods or services to data subjects in the EU for the purposes of Article 3(2)(a)?

(H) Another example would be where a non-EU company offers its EU employees, or those of members of its group, the opportunity to participate in an incentivisation programme. This could either be a monetary or share based incentivisation programme.

(I) If Article 3(2)(a) does apply to these offers there seems to be a risk that non-EU companies may not make employee benefits and incentivisation programmes available to employees within the EU.

(J) This issue also links to the scenario we raise above of offers being made to corporates. Would the non -EU provider of, for example, the concierge service, which contracts with either an EU or non EU corporate be viewed as offering these services to data subjects in the EU?

2.2 Consideration 2(a): offering of goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the Union

Unsolicited sales

(A) The Guidelines provide some useful commentary on the need for some level of targeting at individuals in the EU. There are some other examples on this topic which it would also be helpful if EDPB could cover.

(B) For example, where an EU data subject contacts a retailer in Japan (despite the retailer not actively targeting EU customers) and the Japanese retailer agrees to sell the data subject a product and send it to them in the EU. In these circumstances the retailer is knowingly selling a product to a data subject in the EU but they were not actively targeting EU customers. The EDPB's view on whether this is covered by Article 3(2) would be helpful.

Provision of a service

(C) The GDPR refers to the offering of a service rather than the provision of that service and these two actions frequently take place at different times. As a

result, the data subject may not be in the EU at the time of the offer of the service but would be in the EU at the time of provision of the service.

(D) For instance, a Canadian insurer offers travel insurance to Canadian citizens for travel to the EU. The Canadian citizen then travels to the EU and, whilst there, they contact the Canadian insurer to obtain emergency assistance under the insurance. The offer of the service was therefore made whilst the data subject was in Canada but the service was provided whilst in the EU. In this scenario, the Canadian entity would be aware that the service would be provided in the EU.

(E) This scenario also frequently arises in the banking sector. For instance, a bank account is offered by a Chinese bank to an individual in China. That individual then relocates to the UK for a period of time and the individual continues to access and transact upon their account. The offer of the service was therefore whilst the individual was in China but its provision would be, in part, whilst in the EU. In this scenario the offer of the banking service would not, necessarily, be made with the knowledge that the individual intended to relocate.

(F) The reverse also arises where an offer is made to an individual in the EU but the service is only provided when the individual is outside the EU. For example, where a purely domestic US airline allows individuals in the EU to buy tickets for an internal US flight. There would clearly have to be the targeting of individuals in the EU as explained in the guidance for Article 3(2) to be triggered, but does the location of the provision of the services outside the EU impact on the application of Article 3(2)(a)?

(G) The distinction between offering and providing services is therefore important in understanding the extent of Article 3(2)(a). We have checked several different language versions of the GDPR, and those all use the concept of "offering services" other than the Italian text. The Italian text instead translates as (with highlighting added): "th*e offering of goods or <u>the provision of</u> services",*

(H) Our understanding, in accordance with Recital 23 and the case law on "directing activity", as referred to in the guidelines[1], is that the controller/processor must intentionally "offer" the goods or services to data subjects in the EU, and that the provision of goods or services is therefore insufficient on its own to engage Article 3(2)(a). EDPB clarification on this point would however be appreciated.

<u>Processors</u>

(I) We would also welcome guidance on how Article 3(2)(a) applies to processors. For example, if a non-EU processor is providing IT support services to a non-EU corporate customer which involves support for individual end users in the EU, would this be offering goods and services to people in the EU (even though they are actually the customers of the corporate controller not the processor)?

[1] As referred to in the guidelines at section 2(b), on p. 15

International transfers

(J) A non-EU controller caught by Article 3(2) cannot use the existing standard contractual clauses for onward transfers, as a number of their provisions refer to the applicable law of the exporter's Member State. Guidance on how controllers who are subject to Article 3(2) should be able to effect such onward transfers would therefore be helpful.

(K) Subject to your response to our comments above regarding offers to corporate entities, an issue with onward transfers also arises where a non-EU controller caught by Article 3(2) receives data from an employee ordering goods or services on behalf of his/her employer. For an onward transfer, the controller cannot in these circumstances rely on the derogation under Article 49(1)(b) in respect of a transfer which is necessary for the performance of a contract with the data subject.

(L) One potential partial solution to this issue has been put forward by the UK's Information Commissioner's Office (ICO) in their guidance on international transfers . This guidance puts forward the concept of "restricted transfers" which are subject to the provisions of Chapter V. The ICO's definition of restricted transfers excludes transfers to importers that are already subject to the GDPR themselves, and also excludes transfers between parts of the same organisation (e.g. between branches of the same entity).

(M) Whilst not a complete solution to the challenge identified above, if the EDPB were to adopt such approach, this may provide a basis for at least some transfers by controllers who are within Article 3(2). It would also provide a partial solution to the international transfer issue identified in 1.2(J) above.

2.3 Consideration 2b: monitoring of data subjects' behaviour

(A) We would welcome further guidance on the extent to which the use of cookies constitutes behavioural monitoring and triggers Article 3(2)(b). In particular, whether the use of first party cookies that improve/tailor website experience for returning users would be sufficient to engage Article 3(2)(b). Guidance on this point would be extremely useful given the prevalence of cookies.

(B) We would also welcome clarification that ad hoc monitoring of IP addresses and device fingerprinting by a non-EU controller (or processor) to detect website access from outside their home jurisdiction for the sole purpose of fraud prevention, does not trigger Article 3(2)(b). In such case, the fact that the user happens to be in the EU we view as entirely incidental such that Article 3(2)(b) should not apply.

3. Representatives of controllers or processors not established in the Union

Liability

(A) Further clarification as to the liability of representatives under the GDPR would be very helpful. For example, paragraph 4(d) of the guidelines is not clear as to the circumstances in which enforcement action would be initiated (and penalties imposed) against a representative rather than against the controller or processor that appointed them.

Lead supervisory authority

(B) We would welcome clarification as to whether or not choosing jurisdiction for an EU representative is tantamount to choosing a lead supervisory authority.

(C) The Article 29 Working Party (A29WP) guidelines for identifying a controller or processor's lead supervisory authority suggest this is not the case and that non-EU controllers need to deal with local supervisory authorities in every Member State they are active in. However, the A29WP guidelines on personal data breach notification recommend notifying the regulator in the jurisdiction of the controller's EU representative in the case of a breach, which seems to suggest that regulator would be a lead supervisory authority. Additional guidance on this would therefore be useful.

Establishment

(D) We are aware that others have questioned the rationale behind the view put forward in the Guidelines that having an EU representative under the GDPR does not lead to a non-EU organisation having an establishment within the EU in accordance with Article 3(1)[2]. We believe the guidance as it stands is correct, as otherwise any organisation caught by Article 3(2) and required to appoint a representative would automatically fall within Article 3(1). It is helpful this has been clarified.

Privacy policy

(E) It would be helpful if Example 19 of the Guidelines referred to the Turkish website's obligation (as data controller) to include the name and contact details of their EU representative (in addition to those of the controller) in the information they make available online to data subjects and in their website privacy policy. This would seem to follow on from the points made in the preceding paragraph[3].

If you would find it helpful to discuss any of these comments then we would be happy to do so. Please contact Jon Bartley by telephone on D: +44 20 3060 6394 or by email at

[2] As stated in section 4 of the guidelines, on p. 20.

[3] See section 4(a) of the guidelines, at p. 21.

jon.bartley@rpc.co.uk, or Rebecca Cousin on D: +44 20 7090 3049 or by email at Rebecca.cousin@slaughterandmay.com, in the first instance.

We hereby consent to the publication of personal data contained in this document.