Bird & Bird LLP
12 New Fetter Lane
London EC4A 1JP
United Kingdom
Tel +44 (0) 20 7415 6000
Fax +44 (0) 20 7415 6111
DX 119 London
twobirds.com

TO: ICANN GNSO Expedited Policy Development Process on the Temporary Specification for gTLD Registration Data team ("EPDP team")
FROM: Phil Bradley-Schmieg & Ruth Boardman, Bird & Bird LLP
DATE: 9th September 2019
RE: "Batch 1" of GDPR questions regarding a System for Standardized Access/Disclosure ("SSAD")

QUESTIONS 1 & 2: LIABILITY, SAFEGUARDS, CONTROLLER & PROCESSOR

INTRODUCTION

a) In response to EU regulatory concerns regarding WHOIS and RDAP arrangements' compatibility with EU data protection legislation, ICANN org and the wider stakeholder community have been examining solutions that would allay those concerns, particularly with regard to the EU General Data Protection Regulation 2016/679 ("GDPR").

b) gTLD Registration Data processed by ICANN org and Contracted Parties ("CPs") can be of significant value to third parties ("Requestors"). Requestors may, for example, include security researchers, journalists, law enforcement agencies ("LEAs"), and civil parties investigating or bringing claims for breach of their rights (for instance in intellectual property or defamation matters).

c) Not all gTLD Registration Data will continue to be publicly accessible. There is, therefore, a need to determine how third party requests for non-public gTLD Registration Data will be handled. The European Commission has urged ICANN and the community to develop and implement develop a unified access model that applies to all registries and registrars and provides a stable, predictable, and workable method for accessing non-public gTLD registration data", in the "shortest timeframe possible."[1]

1. QUESTIONS & SAFEGUARDS

1.1 The EPDP team has asked a number of linked questions, with a common set of assumptions. The assumptions are that:

1.1.1 CPs are contractually required by ICANN org to disclose gTLD Registration Data, including personal data, to Requestors;

1.1.2 data must be disclosed over RDAP to Requestors;

[1] Letter from Pearse O'Donohue to Göran Marby, published 3 May 2019; available at https://www.icann.org/en/system/files/correspondence/odonohue-to-marby-03may19-en.pdf

1.1.3 data will be disclosed to Requestors either directly or through an intermediary request accreditation/authorization body;[2]

1.1.4 request accreditation (and/or, we assume, authorization) is carried out by one or more third parties commissioned by ICANN org, without CP involvement;

1.1.5 disclosure takes place in an automated fashion, without any manual intervention; and

1.1.6 data subjects will be duly informed, according to ICANN org's contractual requirements, of the purposes for which, and types of entities by which, personal data may be processed. A CP's contract with ICANN will require the CP to notify data subjects about this potential disclosure and third-party processing before the data subject enters into the registration agreement with the CP, and again annually via the ICANN-required registration data accuracy reminder. The CP can be assumed to have done so.

1.2 We are further told to assume that the SSAD is subject to the following safeguards:

1.2.1 ICANN org or its designee has validated/verified the Requestor's identity, and required in each instance that the Requestor:

1.2.1.1 represents that it has a lawful basis for requesting and processing the data,

1.2.1.2 provides its lawful basis,

1.2.1.3 represents that it is requesting only the data necessary for its purpose,

1.2.1.4 agrees to process the data in accordance with GDPR, and

1.2.1.5 agrees to EU standard contractual clauses for the data transfer.

1.2.2 ICANN org or its designee will log requests for non-public registration data, regularly audit these logs, take compliance action against suspected abuse, and make these logs available upon request by the data subject.

1.3 Against this background, the EPDP team has asked the following questions :

1.3.1 What risk or liability, if any, would the CP face for the processing activity of disclosure in this context, including the risk of a third party abusing or circumventing the safeguards?[3]

1.3.2 Would we deem the criteria and safeguards outlined above sufficient to make disclosure of registration data compliant? If any

[2] Although it was not expressly stated, we assume that the data is disclosed by CPs on a case-by-case basis, in response to incoming requests from Requestors – rather than CPs giving a copy of *all* their gTLD Registration Data to the "intermediary request accreditation/authorization body" in anticipation of receiving requests from Requestors (and then not being involved at all in the fulfilment of those requests).

[3] Your "Question 2", also covered these aspects; for efficiency, it has therefore not been quoted or answered separately.

risk exists, what improved or additional safeguards would eliminate this risk?

1.3.3 In this scenario, would the CP be a controller or a processor, and to what extent, if at all, is the CP's liability impacted by this controller/processor distinction?

1.3.4 If a risk still exists for the CP, what additional safeguards might be required to eliminate CP liability depending on the nature of the disclosure request, i.e. depending on whether data is requested e.g. by private actors pursuing civil claims or law enforcement authorities depending on their jurisdiction or the nature of the crime (misdemeanour or felony) or the associated sanctions (fine, imprisonment or capital punishment)?

1.4 A CP's liability under the GDPR is significantly affected by whether it is a "controller" or a "processor". We therefore address the question set out at paragraph 1.3.3 above first. As liability is also affected by the extent to which safeguards effectively meet legal obligations, we have considered this question second, before addressing liability (and ways of removing liability) last.

2. ARE THE CPS ARE CONTROLLERS OR PROCESSORS IN THIS SCENARIO?

2.1 As the EPDP team will be aware, the GDPR distinguishes between entities that are "controllers" and "processors".

"Controllers"

2.2 The "controller" is the "*natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*" (GDPR Article 4(7)).[4]

2.3 This is a factual determination: entities cannot assign or disclaim controller status. Unless this status is assigned by law, the status flows from actual control over key data processing decisions.

2.4 Guidance on this was provided in 2010 by the Article 29 Working Party ("WP29", the body which was formally tasked with preparing EU-wide guidance on EU data protection law until May 2018, when it was replaced by the European Data Protection Board, "EDPB"). The WP29 took the view that "*the first and foremost role of the concept of controller is to determine who shall be responsible for compliance with data protection rules, and how data subjects can exercise the rights in practice. In other words: to allocate responsibility.*"[5] Read literally, this reflects that a controller has responsibility for most obligations under the GDPR; but the phrase also indicates a degree of regulatory expediency: it shows the underlying need to hold someone accountable. This can influence a court or supervisory authority's approach.

---

[4] The GDPR also contemplates that "*where the purposes and means of such processing are determined by [EEA] or Member State law, the controller or the specific criteria for its nomination may be provided for by [EEA] or Member State law*". We are not aware of any legislation that assigns controller status to ICANN org or the CPs.

[5] WP29, *Opinion 1/2010 on the concepts of "controller" and "processor"* ("WP 169"), at p. 4. Available online at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf . Note that this guidance dates from 2010 and thus predates both the GDPR and the case law cited later in this section. It is currently being revised by the EDPB, which may bring greater clarity and consistency.

"Processors"

2.5 A processor is the "*natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller*". According to the WP29, a processor serves "*someone else's interest*" by "*implement[ing] the instructions given by the controller at least with regard to the purpose of the processing and the essential elements of the means*".[6]

2.6 The guidance pays particular attention to '*the degree of actual control exercised by a party, the image given to data subjects and the reasonable expectations of data subjects on the basis of this visibility*".[7] There is recognition that a processor can have significant freedom to determine technical and organisational aspects of the processing.[8] However, WP169 explains there are essential elements that are traditionally and inherently reserved to the determination of the controller, such as *'which data shall be processed?', 'for how long shall they be processed?',* and *'who shall have access to them*?' An entity that makes such decisions is acting as a controller, not a processor.[9]

2.7 An entity can be both a controller and processor. This will be the case where an entity that acts as a processor also makes use of personal data for its own purposes: the WP29 gives the example of a service provider, entrusted with data for processing purposes, also using it for its own benefit, and thereby being a controller over that other activity.[10] A significant consequence of being a processor is that the entity can only process personal data pursuant to instructions of the controller(s), or as required by EEA or Member State law.[11]

Application to the SSAD

Presumption of controllership

2.8 In WP169, the WP29 suggests that organisations fulfilling certain roles will, as a consequence, automatically be regarded as controllers. It states that *"rules of thumb and practical presumptions are needed to guide and simplify the application of data protection* law*"* and that in many situations there will be "*circumstances from which factual influence can normally be inferred, unless other elements indicate to the contrary"*[12]. In particular:

"*This is the case where the capacity to determine is not explicitly laid down by law, nor the direct consequence of explicit legal provisions, but .. stems… from established legal practice pertaining to different areas… In this case, existing traditional roles that normally imply a certain responsibility will help identifying the controller: for example, the employer in relation to data on his employees, the publisher in relation to data on subscribers, the association in relation to data on its members or contributors".*

The relation between CP and registrant (or registrants contact) could be regarded in a similar way.

---

[6] *Ibid*., at p. 25
[7] *Ibid*., at p. 32.
[8] *Ibid*., at p. 14.
[9] *Ibid*., at p. 14.
[10] *Ibid*., at p. 14.
[11] See GDPR Articles 28(3) and 29.
[12] WP169, p.9

2.9 In similar manner, the WP29 emphasizes consideration of "*the image given to data subjects and the reasonable expectations of data subjects on the basis of this visibility*". A person who registers a domain name with a CP and provides his or her details to that CP (or whose employer registers the domain name, then lists that data subject as an administrative or technical contact), will – we assume – typically expect that the CP will be a controller for the CP's disclosure of their data to third parties (whether the disclosure is direct, or using a third party platform). Traditionally, CPs have been seen as the controller of this particular activity.[13] This will lead to a presumption that CPs continue to be controllers, even once an SSAD is implemented.

Difficulty presenting CPs as acting "on behalf of" someone else

2.10 The WP29 emphasizes that "*the most important element [in the definition of processor] is the prescription that the processor act 'on behalf of the controller…' Acting on behalf means serving someone else's interest…*" Related to the likelihood that authorities (and data subjects) will assume that a CP is a controller, is the difficulty of showing that the CP is only serving ICANN's interest and processing personal data on ICANN's behalf. Having to disclose information to Requesters is likely to be seen as an inevitable consequence of being a CP – rather than something a CP has agreed to do on ICANN org's behalf. The fact that a CP would presumably still have to disclose data directly to Requestors if ordered to do so (by order of a court or other authority), reinforces this.

A move away from a macro, presumptive analysis toward close analysis of technical processing activities

2.11 We are asked to assume that ICANN will have significant control over the operation of the SSAD and, hence, the disclosure of data by the CPs. WP169 does note that where there is an assumption that a person is a controller (referred to in WP169 as "*control stemming from implicit competence*") that this should only be the case "*unless other elements indicate the contrary*". We have considered if a close analysis of the facts would lead to a different outcome. Recent cases from the CJEU – in particular its recent *Fashion ID* ruling – have also supported closer, fact-specific analysis.[14]

2.12 However, these cases suggest that there is a low threshold to become a controller. The test, according to the CJEU, is simply whether someone "*exerts influence over the processing of personal data, for his own purposes, and (…) participates, as a result, in the determination of the purposes and means of that processing*".[15]

2.13 The low bar, so far as determination of *purpose* is concerned, is illustrated by *Fashion ID*, where the deliberate use by one controller (*i.e.* the website operator) of a system provided by another (*i.e.* Facebook), to their mutual benefit, was held to be "participation" by the operator in determining the "purpose" of Facebook's personal data collection from visitors to the operator's website – even though the operator did not directly benefit from that personal data processing, but rather, from greater visibility of its content on Facebook.[16]

---

[13] See Appendix C to the Temporary Specification: https://www.icann.org/resources/pages/gtld-registration-data-specs-en/#appendixC

[14] Judgement of the CJEU in Case C-40/17 *Fashion ID*, at [74].

[15] *Ibid.*, at [68].

[16] "*The reason why Fashion ID seems to have consented, at least implicitly, to the collection and disclosure by transmission of the personal data of visitors to its website by embedding such a plugin on that website is in order to benefit from the commercial advantage consisting in increased*

2.14 The *Jehovan Todistajat* ruling exemplifies a similarly low bar in relation to determination of the "means": the Jehovah's Witnesses community was stated to have "general knowledge" and to have encouraged and coordinated data collection by community members at a very general level – but it was nevertheless held to have satisfied the test for controllership.[17] In *Fashion ID*, it was sufficient for the website operator to integrate with Facebook platform code, such that the operator thereby participated in determination of the "means" of Facebook's data collection.[18] Courts and supervisory authorities are likely to consider that a CP is involved in determination of the means of processing, possibly merely by virtue of implementing/interfacing with the SSAD – drawing parallels with *Fashion ID*.

Factors that could lend support for processor status

2.15 As mentioned at paragraph 2.6 above, the WP29 notes that '*the degree of actual control exercised by a party, the image given to data subjects and the reasonable expectations of data subjects on the basis of this visibility*" are important.[19]

2.16 The assumptions make clear that CPs will be required by contract to disclose Registration Data to requestors over RDAP. Although it is not mentioned in the assumptions, our understanding from separate, earlier, discussions with the EPDP team is that ICANN takes steps to monitor compliance with this type of contractual commitment. As the WP29 makes clear, this can be proof of a controller-processor relationship, since "[*a] constant and careful supervision by the controller to ensure thorough compliance of the processor with instructions and terms of contract provides an indication that the controller is still in full and sole control of the processing operations*".

2.17 The safeguards could also result in individuals becoming more aware of ICANN's role in this processing – in particular if the domain name registration process and annual data accuracy reminder clearly present the collection of this data (and its eventual input into SSAD) as something that is done (only) on ICANN org's behalf. ICANN org website materials, and other presentational factors (e.g. privacy notices etc.) would also have to clearly depict this activity as being performed by CPs solely on ICANN org's behalf.

Summary – CPs most likely to be joint controllers with ICANN

2.18 We consider that the most likely outcome – and certainly most supervisory authorities' starting position – is that CPs are controllers – and, given ICANN's role in determining purposes and means of processing, that they will be joint controllers with ICANN org in respect of their disclosure of Registration Data to Requesters via a SSAD.

---

publicity for its goods; those processing operations are performed in the economic interests of both Fashion ID and Facebook Ireland, for whom the fact that it can use those data for its own commercial purposes is the consideration for the benefit to Fashion ID. (…) In such circumstances, it can be concluded (…) that Fashion ID and Facebook Ireland determine jointly the purposes of the [collection of that data by Facebook]." *Ibid.*, at [80-81].

[17] Judgement of the CJEU in Case C-25/17 *Jehovan Todistajat*, at [73].

[18] "*Fashion ID appears to have embedded on its website the Facebook 'Like' button made available to website operators by Facebook Ireland while fully aware of the fact that it serves as a tool for the collection and disclosure by transmission of the personal data of visitors to that website, regardless of whether or not the visitors are members of the social network Facebook. (…) Moreover, by embedding that social plugin on its website, Fashion ID exerts a decisive influence over the collection and transmission of the personal data of visitors to that website to the provider of that plugin, Facebook Ireland, which would not have occurred without that plugin.*" *Ibid.*, at [77-78].

[19] *Ibid.*, at p. 32.

2.19 The European Data Protection Board ("EDPB") is working on a new Opinion on controller/ processor status, to update and replace WP169 and this is anticipated in the next 6 months. This will be highly influential, so it will be important to assess it, once it materialises. If CPs and ICANN consider strongly that joint controller status is incorrect, then thought could be given as to whether to seek to actively engage with those involved with the guidance, in pursuit of new guidance that might help the case for CP processor status here. There is, of course, no certainty that the authorities responsible for the guidance would be amenable to such outreach, or that it would have a positive outcome for CPs.

3. ARE THE SAFEGUARDS PROPOSED SUFFICIENT TO MAKE DISCLOSURE OF REGISTRATION DATA COMPLIANT?

What must the safeguards address?

3.1 A controller is responsible for compliance with all aspects of the GDPR, whereas only certain provisions of the GDPR are applicable to processors. The difference can be shown as summarised below:

GDPR Obligation	Controller	Processor
Lawfulness and Transparency of Processing		
Data Quality		
Data Minimisation		
Data Retention		
Security		
Accountability (i.e. demonstrating compliance with above principles)		
Compliance with Individual Rights		
Data Protection by Design and by Default		
Cooperate with Data Protection Authority		
Notification of Security Breaches		
Data Protection Impact Assessments		
Appointment of DPO		
Records of Processing		
Data Transfers		

Red = Direct obligation
Yellow = GDPR requires the processor be obliged by contract to assist the controller

3.2 Where parties are joint controllers, this does not mean that the parties each have to undertake all elements of compliance. In *Wirtschaftsakademie* the CJEU states [75] that "*the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case*"[20]. The case considered joint control under the Data Protection Directive and the GDPR Art.26 now requires that joint controllers must "*determine their respective responsibilities for compliance… in particular as regards the exercising of the rights of the data subject and their respective duties to provide .. information.. by means of an arrangement between them…*".

[20] Case C-210/16

3.3 As can be seen from the table above, controllers, rather than processors, face the greatest compliance challenges and risks of liability under the GDPR. Even so:

3.4 when processing is undertaken by a processor, then this must be governed by a contract which must contain the content set out in GDPR Art.28;

3.5 if a processor suspects that a controller's instructions to it (e.g. to disclose personal data) would result in unlawful data processing, then the terms of the processor's contract will require it to report those beliefs to the controller without delay; and

3.6 a processor that processes personal data (or subcontracts that processing) either in breach of its contract or otherwise in a manner inconsistent with the instructions of the controller, can become a controller itself, and thus face liability for the sorts of breaches identified in column 2 of the table at paragraph 3.1 above.

SSAD safeguards

3.7 Under the SSAD, we understand that a CP has no means to individually review and then modify, approve or deny SSAD requests; instead, the system is automated, and key parts of the process are entrusted to ICANN org (or its designee, if any). Accordingly, a CP is reliant on the system's design and safeguards for assurance that the processing will meet GDPR requirements.

3.8 The SSAD would need to accommodate requests for Registration Data from a wide variety of requestors from different countries, with different legal powers (in some cases) and interests. It would also need to meet the obligations of CPs in different countries, again, subject to a variety of different legal requirements. Even were the analysis to be limited to the requirements of the GDPR alone, this would require considerable time, due to the variety of requests which could be received. Accordingly it is not possible to confirm, in this note, that the criteria and safeguards described would be sufficient to make disclosure of registration data compliant. At a general level, the safeguards the EPDP team has described are helpful, but will, at least, also need to include measures to address the points described below.

<u>Legal basis</u>

3.9 The safeguards require attestation by the Requestor that it has a legal basis for its collection of personal data via the SSAD. Our conclusion above is that CPs will most likely be viewed as controllers for this processing. Accordingly, the main concern for CPs will be that *they* (rather than a Requestor) have a legal basis for the processing. Where multiple different controllers are involved, the challenge is greater.[21]

3.10 In some cases, compliance with a request may be legally mandatory or expressly authorised, in either case under EEA/Member State law – but that will vary on a case by case basis (e.g., depending on where a CP is based). The SSAD rules would need to be capable of taking account of the legal framework particular to a given CP.

3.11 In other cases, the CP may instead rely on legitimate interests. Here the SSAD safeguards would have to ensure that the interests of a disclosure have been assessed against the risk of negative effects for the data subject(s):

[21] In case C-40/17 *Fashion ID*, at [96], the CJEU appeared to confirm that each joint controller must have a legal basis for processing under their joint control – seemingly ruling out any arguments that they can both rely on just one responsible controller having a legal basis.

3.11.1 As the EPDP team itself has flagged, the nature of the disclosure request,[22] is important here.

3.11.2 Significant care would need to be taken to pre-assess and balance the legitimate interests so as to streamline their consideration. This could be true even where requests are categorised based on the sorts of distinction of which the EPDP has provided examples: one category of request might be "requests from law enforcement bodies investigating crimes carrying a sentence of [x] years of more" – and yet it might not be safe to assume that for such a bucket, the balance of legitimate interests is *always* in favour of disclosure, as this could be affected by the status of the data subject or the country in which the law enforcement body is located.

3.11.3 Investigations that could lead to capital punishment (mentioned in your question) are particularly sensitive, since capital punishment is prohibited under the EU Charter of Fundamental Rights; further research (not conducted for present purposes) would be required in order to determine whether the GDPR could nevertheless tolerate processing of personal data in such contexts.[23]

3.11.4 It would be helpful if the safeguards included assurances that improper volumes of data will not be disclosed to requesters – we note that a declaration (for each request) will be made by the Requestor (but this many not always be reliable).

3.11.4.1 Automated, rules-based monitoring and blocking of unusual request sizes or volumes could be considered. (This may already have been envisaged by the safeguard mentioned at paragraph 1.2.2 above, but that is not clear.)

3.11.4.2 It would help to consider (at the design stage) what fields could safely be disclosed for different types of request – similar to "need to know"/"role-based access" permissioning systems in IT more generally.

3.12 We have commented in further detail on factors to consider when balancing the legitimate interests of the relevant parties and those of the individual in our note in response to question 4. That note also considers that some level of meaningful human review will still be needed in order to avoid an entirely automated system amounting to automated individual decision-making, as regulated by art.22 of the GDPR.

<u>Individual rights</u>

3.13 The safeguards will need to address how data subject requests will be met.

---

[22] You mentioned different scenarios, e.g. requests "*by private actors pursuing civil claims or law enforcement authorities depending on their jurisdiction or the nature of the crime (misdemeanor or felony) or the associated sanctions (fine, imprisonment or capital punishment)*"

[23] Capital punishment is prohibited under the EU Charter of Fundamental Rights, Article 2(2). The GDPR must be interpreted in a manner compliant with the EU Charter. Accordingly, it may be that under the GDPR, personal data processing can never be "lawful", "fair" and/or in the overriding legitimate interests of a controller, in situations where the processing would foreseeably expose the data subject to capital punishment. The UK court has rejected a similar argument in *The Queen (on the application of Maha El Gizouli) v Secretary of State for the Home Department* [2019] EWHC 60 Admin. However, the court was clearly influenced by the facts of the specific case and the decision has difficulties.

3.14 *Access right*: delivery of request logs to a data subject (mentioned at paragraph 1.2.2 above) will go part of the way towards complying with GDPR Article 15 (a data subject is entitled to information about recipients of her/his data). Logs showing what data has been requested about a data subject, may themselves be personal data – perhaps quite high risk/sensitive, if for instance they indicate that someone is a person of interest in in criminal or civil investigations. This entails strict security measures around their storage and availability (including how to check that a person wishing to see this information, is in fact the data subject).

3.15 There will also be a need to consider:

3.15.1 how many years' worth of such data to hold and provide access to (the CJEU has in the past emphasised the importance of data subjects being able to find out who, historically, has accessed their data; but also noted that this is not absolute, and the number of years' worth of request data someone can obtain could be limited (in that case, by law), and can be balanced against storage limitation/data minimisation considerations, plus inconvenience to the data controller).[24]

3.15.2 how the rest of the information and/or copies of personal data required by Article 15 will be provided; and

3.15.3 how to deal with cases where the provision of some or all of this data would be resisted by Requestors, e.g. law enforcement authorities seeking to avoid tipping off subjects of investigations. EEA Member State law typically provides exemptions for GDPR access and notice rights in those cases, but these are not harmonised, and thus could vary based on applicable jurisdictions (of a CP and/or of a Requestor and/ or a data subject).

3.16 *Other rights:* There safeguards will need to consider other forms of data subject request; for instance demands to restrict (i.e. freeze) or block all processing of personal data relating to a given data subject.

Data transfer

3.17 In respect of international data transfer safeguards, we note that the EPDP envisages relying on the EU Standard Contractual Clauses (SCCs). However:

3.17.1 the EPDP should anticipate that some Requestors, especially public authorities, will not agree to be bound by their terms;

3.17.2 the terms of the SCCs are not always easy to comply with, especially when SCCs are used at scale. In particular, under the 2004 version of the SCCs, the data exporter must warrant that it "*has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses*"[25]. A process will need to be in place to conduct this diligence;

3.17.3 lastly if EEA based CPs were to be processors, this would somewhat complicate reliance on the SCCs in order for CPs to export data to ICANN org or Requestors outside the EEA; all forms of SCC available today are premised on the data exporter being a controller established in the EEA. It

[24] Case C-553/07 *Rijkeboer*.
[25] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0915

may be the case that ICANN's Brussels establishment is able to serve in this capacity.

Security

3.18 Data security safeguards will need to be appropriate to the risks that data subjects will be exposed to, should the confidentiality, integrity or availability of the data be compromised. We also note that any processors selected to help run the SSAD will need to be appointed and managed according to the GDPR's stringent requirements.

4. WHAT RISK OF LIABILITY WOULD THE CP FACE FOR DISCLOSURE, INCLUDING AS A RESULT OF THE REQUESTER ABUSING OR CIRCUMVENTING SAFEGUARDS. HOW COULD RESIDUAL RISK BE ELIMINATED?

4.1 As regards the extent of liability should safeguards be held to be inadequate, or circumvented by Requestors, it is helpful to distinguish between liability to individuals (e.g., civil lawsuits), and liability to enforcement action by supervisory authorities (e.g., fines).

Liability to individuals

4.2 Article 82, subsections (2)-(4), set out the rules on liability to individuals:

"2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject."

4.3 Under these provisions, joint and several liability is not limited to joint control scenarios: it is the principle whenever parties (of any description) are involved in the "same" processing.[26] GDPR art.82(5) sets out a statutory right to recover an appropriate amount of the compensation that was paid out, from those other parties.

4.4 If CPs are processors, they will only be liable under art. 82 if they have failed to comply with obligations placed on processors under the Regulation, or have acted outside or contrary to lawful instructions from the controller. Were courts or supervisory authorities to accept that CPs are processors, then it seems unlikely that CPs would breach the controller's instructions, given the SSAD is automated. Their most likely source of liability would therefore concern security shortcomings or failure to comply with the GDPR's international data transfer rules; CPs might

[26] For joint controllerships, GDPR Article 26(3) adds that where parties are joint controllers, "*the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers*". This would include rights such as the rights of access and objection as well as the right to claim compensation under Article 82.

therefore look to ICANN org to prescribe security and international data transfer arrangements – giving CPs more scope to argue that, for the purposes of art.82(3), they are "*not in any way responsible for the event giving rise to the damage*".

4.5 If the CPs are controllers, and if a disclosure infringes the GDPR, they are unlikely to be able to avoid liability to individuals. Firstly, it will be more difficult to avoid *all* liability under Article 82 by proving that the CPs are "*not in any way responsible for the event giving rise to the damage*" – the "event" in question may well be held to be the actual disclosure, which CPs participate in actively, rather than (for instance) improper assessment of a Requestor's identity or its grounds for accessing the data.

4.6 The existence of *any* liability under Article 82 would then potentially expose a CP to liability for *all* the damage suffered by the data subject, on a joint and several liability basis. To avoid this, it would need to prove that it was not involved in "*the same processing*". In particular, the likelihood of joint and several liability of CPs with other parties will be greatest if they are joint controllers, as it is particularly likely that in those cases they will be seen as involved in the "same" processing and this is re-enforced by art.26(3) on joint control, which provides that (irrespective of any joint control arrangement) "*the data subject may exercise his or her rights under this Regulation* [including to compensation*] in respect of and against each of the controllers".*

4.7 CPs held to have joint and several liability to individuals for all damage suffered by data subjects, would then in turn need to reclaim appropriate contributions from other responsible parties, under GDPR Art. 82(5). CPs may instead be able to seek the other parties' joinder directly to the proceedings brought by the data subject, in which case the Court may apportion responsibility between them directly.[27]

4.8 As remarked in the questions you raised, the Requestor might be one of those parties, if it has abused the system in order to gain improper access to data. The next section explores this in more detail

GDPR breaches caused by a Requestor

4.9 Article 32 requires both controller and processor to take appropriate "*technical and organisational measures*" to protect the confidentiality of the data. Article 32(2) specifically calls out the need to take account of the risks posed by unlawful or unauthorised access to personal data. Accordingly, ICANN and the CPs have a positive obligation to address the risk posed by those seeking improper access to personal data for which they are responsible and they could face *primary* liability to individuals for that breach. By way of example of this, the monetary penalty imposed by the Information Commissioner, under the UK's now-repealed Data Protection Act 1998, on Facebook in respect of Cambridge Analytica's misuse of data shows that security obligations can be held to include a positive obligation to guard against improper use of data by its eventual recipients[28].

4.10 However, GDPR security obligations are not absolute; they must only be "*appropriate*" to the level of risk. Despite a safeguard's circumvention by a

[27] GDPR Recital 146 suggests that if those other parties can be joined to the data subject's proceedings against the CP, the court "may" apportion liability between them there and then, rather than holding any given party liable for the whole amount on a joint and several basis. However, the Recital adds that this would have to be "in accordance with Member State law", which might vary from case to case.
[28] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/ . Note however that this fine is under appeal by Facebook; see https://www.bbc.com/news/technology-46292818

Requestor, a court might therefore accept that safeguards were adequate (or that the defect, if any, was so minor that only a small amount of a data subject's claimed damages would be attributable to those shortcomings).

4.11 There is also a possibility that ICANN org and the CP may be deemed to be "*involved in the same processing*" as the Requestor, and thus jointly and severally liable with the Requestor. Depending on the circumstances, ICANN org and/or the CP may be able to counter that despite being "*involved in the same processing*", they are nevertheless "*not in any way responsible for the event giving rise to the damage*" for the purposes of art. 82(3) purposes, and thus not subject to GDPR Art. 82(4) joint and several liability. Should that fail, they would need to seek to either (i) recover the compensation they pay (or a portion thereof) from the Requestor, or (ii) join the Requestor to the primary proceedings, and seek apportionment of damages directly.

Liability to supervisory authorities

4.12 Supervisory authorities are able to take action against controllers and processors. This liability, just as with liability to individuals, could potentially apply whether the processing is carried out by the controller or processor itself, or subcontracted to another entity.

4.13 Unlike liability to individuals, however, it is less clear that a strict joint and several liability principle applies whenever multiple parties are involved in "*the same*" processing. On the contrary, there is scope to argue that enforcement action (including but not limited to fines) should not be imposed if and to the extent that the infringement is allocable to the actions of another party involved in the processing:

4.13.1 when imposing fines, GDPR Article 83(2)(d) requires the authority to take into account "*the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 [privacy by design] and 32 [security]*";

4.13.2 there must generally be clear wording to impose joint and several liability – so this would need to be expressly set out to be the case. The GDPR did this expressly as regards actions by individuals (under Article 82), so this strengthens the argument that this would have been stated expressly if it was intended in respect of fines from supervisory authorities;

4.13.3 from a policy perspective, it makes sense to provide for joint and several liability as regards individuals who, absent that provision, may struggle to obtain compensation due to difficulties of proving responsibility between connected parties. However, the same policy objective does not apply here, so far as supervisory authorities are concerned – as Art. 83(2)(d) makes clear;

4.13.4 even when parties are deemed to be joint controllers, recent court decisions (concerning enforcement by supervisory authorities) have emphasised that joint control does not imply equal responsibility for breaches of the GDPR.[29] Whilst this cannot override clear GDPR provisions to the contrary (e.g. GDPR provisions on joint and several liability to individuals), it would likely be influential in the *absence* of that clear wording, as is the case here.

4.14 CPs, as joint controllers with ICAN org, would therefore likely benefit from clear allocation of responsibilities to the other part(y/ies), so far as possible, under the

[29] Case C-40/17 *Fashion ID*, at [70], also citing *Jehovan Todistajat*.

terms of the joint controllership “arrangement” they must enter into pursuant to GDPR Art. 26.

4.15 For the sake of completeness, we note that it *may* also be possible to use the "lead authority"/ co-operation and consistency provisions under Chapter IV of the GDPR so as to ensure that enforcement by supervisory authorities takes place against ICANN org's Brussels establishment, rather than against CPs. In broad terms, these provisions provide a streamlined mechanism for controllers and processors to deal with supervisory authorities, in situations where multiple supervisory authorities would otherwise be involved.

4.16 Where a lead authority is competent, then it is to be the "*sole interlocutor*" of the controller or processor (art.56(6)). However, an additional benefit of having a lead authority is that there should only be enforcement by the lead authority. Although not explicitly stated, this is implicit in art.60, which provides that any decision against a controller or processor has to be taken by the lead authority and that that decision will then be binding on all other authorities. Both Recitals 135 and 138 confirm this by providing that the consistency mechanism under the one-stop-shop principle "*should […] apply where a supervisory authority intends to adopt a measure interned to produce legal effects […]."*

4.17 This co-operation and consistency process is only available where there is "cross border processing" of personal data, which is the case where:

4.17.1 processing of personal data takes place in the context of the activities of establishments of a controller or processor in more than one member state; or

4.17.2 processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Accordingly, whether the procedure applies may depend on the facts. The procedure could (subject to the point below) be available in the event of a deficiency in the SSAD which is systemic, or which otherwise affects individuals in multiple member states. However, if there were to be a one-off breach of the GDPR, which only affected an individual in one member state then this would not be cross border processing so the procedure would not be applicable. Article 66 also allows supervisory authorities to take provisional measures at national level (so by-passing the lead authority procedure) in the event of an urgent need.

4.18 Articles 56 and 4(16) of the GDPR set out which supervisory authority will be the lead authority for a controller and for a processor. However, they do not address the situation of joint control. The relevant WP29 guidelines note that there is no provision in the GDPR for a lead authority for joint controllers, however, it goes on to suggest that “*to benefit from the one-stop-shop principle, the joint controllers should designate (among the establishments where decisions are taken) which establishment of the joint controllers will have the power to implement decisions about the processing with respect to all joint controllers. This establishment will*

then be considered to be the main establishment for the processing carried out in the joint controller situation."[30]

4.19 Accordingly, if ICANN org's Belgian establishment were to be "*designated*" by the parties in the manner suggested by the guidance above, then this might help further minimise the risk of enforcement directly against CPs in other EEA Member States (at least in non-urgent cases that have a cross-border dimension).

4.20 This is a novel and (so far as we are aware) untested approach. The guidance cited above has no basis in the text of the GDPR (the guidance itself notes that "*the GDPR does not specifically deal with the issue*"). Accordingly, if this suggestion is of interest, it would be important to discuss it further with supervisory authorities.

[30] Article 29 Working Party, *Guidelines for identifying a controller or processor's lead supervisory authority* (WP 244), at [2.1.3]. Available online at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235