**Executive Summary:**

The EPDP Phase 2 team sent its first batch of questions to Bird & Bird on 29 August 2019. Bird & Bird answered this batch of questions in a series of three memos. [Memo 1](https://community.icann.org/download/attachments/117604842/ICANN-EPDP%20-%20Qs%201%20%26%202%20-%209th%20September%202019%5B2%5D.pdf?version=2&modificationDate=1568143518000&api=v2) was delivered on 9 September 2019. Memo 1 analyzed the legal role of contracted parties in the proposed System for Standardized Access/Disclosure (SSAD), the sufficiency of the proposed safeguards, and the risk of liability to contracted parties for disclosure via the SSAD. The questions sent to Bird & Bird are provided in the Annex to this document and include a series of assumptions in Section 1.1 and 1.2 that are part of the factual basis for the responses below.

In response to these questions, Bird & Bird noted the following with respect to controllership:

1. Contracted parties are likely controllers in the SSAD since registrants have traditionally reasonably expected that contracted parties are the controller for disclosure of their data to third parties. It is difficult to show that contracted parties are only serving ICANN org’s interests, particularly in light of relevant judicial decisions that suggest a low threshold for controllership.
2. If the EPDP Team wanted to recommend a policy under which contracted parties are processors in a SSAD, steps could be taken to support this policy goal. Contracted parties would need to have no substantial influence over key aspects of SSAD data processing, such as (i) which data shall be processed; (ii) how long shall they be processed; and (iii) who shall have access to the data. There would also be a need for “constant and careful” supervision by ICANN org “to ensure thorough compliance of the processor with instructions and terms of the contract”, and efforts to instruct registrants that contracted parties are only acting on ICANN org’s behalf (e.g., ICANN org website materials, privacy notices, information in domain name registration process).
3. However, the most likely outcome and starting position for supervisory authorities would be that contracted parties are controllers and likely joint controllers with ICANN org regarding disclosure of registration data through the SSAD.

Bird & Bird noted the following with respect to SSAD safeguards and liability:

1. Given the number of jurisdictions involved, and the likely variety of requests that could be handled by the SSAD, Bird & Bird could not confirm that the criteria and safeguards described in the assumptions would make disclosure of data in a fully automated SSAD compliant.
2. Bird & Bird suggested additional safeguards that the EPDP should consider related to (i) legal basis, proportionality, and data minimization; (ii) individual rights; (iii) international data transfer; and (iv) security.
3. Under the GDPR, parties involved in the same processing are subject to liability to both individuals and supervisory authorities. Individual liability is joint and several, meaning each party involved in the processing is potentially liable for all damages to the data subject, with some differing standards for controllers vs. processors. Supervisory authorities may proceed against controllers or processors, and it is currently unclear whether joint and several liability applies when multiple parties involved in the same processing (i.e., enforcement action isn’t appropriate if others are responsible).

**1. Are Contracted Parties Controllers or Processors?**

***Controllers***

* Liability is significantly impacted by whether Contracted Parties are controllers or processors. (1.4)
* A 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.” (2.2)
* Whether an entity is a controller is a factual determination based on “control over key data processing decisions.” The role of controller cannot be assigned or disclaimed. (2.3)
* The Article 29 Working Party provided pre-GDPR [guidance](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf) on the roles of controller and processor. The EDPB is currently revising this guidance with an update anticipated in the next six months. (2.4, 2.19)
* The EDPB’s predecessor, the Article 29 Working Party (WP29) determined 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.” 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, says B&B. (2.4)
* An entity that makes key decisions (alone, or jointly with others) about (i) what data is processed; (ii) the duration of processing; and (iii) who has access to data is acting as a controller, not a processor – these are sometimes referred to as the "essential elements" of processing. (2.6)
* An entity can be both a controller and a processor. This will be the case where an entity that acts as a processor also makes use of personal data for its own purposes. (2.7)

***Processors***

* A processor is the “natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.” (2.5)
* The Article 29 Working Party guidance emphasizes the importance of examining “'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” in determining whether an entity is a controller or processor. (2.5)
* According to 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.” (2.5)
* A processor can only process personal data pursuant to instructions of the controller or as required by EEA or Member State law. (2.7)

***Application to the SSAD***

*Presumption of controllership*

* In some cases, "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 a Contracted Party and registrant (or registrant's contact) could be regarded in a similar way. (2.8) Similarly, the “image given to data subjects and the reasonable expectations of data subjects” is an important consideration for determining controllership. A registrant will typically expect that Contracted Parties are the controller for disclosure of their data to third parties. (2.9)
* Since Contracted Parties are currently seen as the controller for disclosure of data to third parties, this will lead to a presumption that Contracted Parties continue to be controllers, even once an SSAD is implemented. (2.9)
* However, such a presumption can’t always be made, depending on analysis of technical processing activities. 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". Recent cases from the CJEU – in particular its recent *Fashion ID* ruling – have also supported closer, fact-specific analysis. (2.11)

*Difficulty presenting Contracted Parties as acting “on behalf of” someone else*

* The most important element of a processor’s role is that they only act on behalf of the controller. It will be difficult to show that Contracted Parties are only serving ICANN’s interests and processing data on ICANN’s behalf. (2.10)
* Disclosure of data is likely to be seen as an inevitable consequence of being a Contracted Party, not something that Contracted Parties agree to do on ICANN’s behalf. (2.10)

*Close factual analysis of technical processing activities*

* The factual threshold for becoming a controller (determining purposes or means of processing) is low. 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”. (2.12)
* In the CJEU's *Jehovan Todistajat* ruling, the national Jehovah's Witnesses community organization was stated to have “general knowledge” and to have encouraged and coordinated data collection by community members (door to door preachers) at a very general level – but it was nevertheless held to have satisfied the test for joint controllership with those community members. In the CJEU's *Fashion ID* ruling, 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, and was a joint controller with Facebook. (2.14)
* Courts and supervisory authorities are therefore likely to consider that a Contracted Party is involved in determining the means of processing, possibly just by implementing/interfacing with the SSAD. (2.14)

*Factors that could support processor status*

* The key to avoid controller status is being able to show that you are not involved in determining the "essential elements" of processing (2.6).
* Also, ICANN monitoring compliance with a contractual requirement to disclose data could be proof of a controller processor relationship, since “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.” (2.16)
* Taking steps to clearly inform data subjects that data is collected only on ICANN’s behalf (e.g. disclosures in domain name registration process, annual data accuracy reminder, privacy notices, ICANN org website materials) and other presentations that clearly depict this action as being performed by CPs solely on ICANN’s behalf could result in individuals becoming more aware of ICANN’s role as a Controller, and the Contracted Parties' role as a processor. (2.17)

*Summary – Contracted Parties most likely joint controllers with ICANN*

* The most likely outcome and the starting point for supervisory authorities is that Contracted Parties are controllers. (2.18)
* ICANN’s role in determining purpose and means of processing suggests they are joint controllers with Contracted Parties for the disclosure of data to third parties. (2.18)

**2. Are the Safeguards Proposed Sufficient to Make Disclosure of Registration Data Compliant?**

*SSAD safeguards*

* Given the number of jurisdictions involved, and the likely variety of requests that could be handled by the SSAD, this opinion cannot confirm that the criteria and safeguards described in the assumptions would make disclosure of data in a fully automated system compliant. (3.8)
* B&B states that care must be taken in processing personal data -- a processor (either in breach of its contract with the controller or otherwise behaving in a way inconsistent with the instructions of the controller) can become a controller itself, and thus face breaches (as identified in the table on p.7 of the memo). (3.6)
* The safeguards described are helpful, but will need to include additional measures described below. (3.8)
	+ Legal basis: safeguards need to (i) consider whether Contracted Parties, not just Requestor, have a legal basis for processing; (ii) account for the particular legal framework applicable to a Contracted Party; (iii) ensure that an appropriate balancing test is performed on legitimate interests, if that is an appropriate legal basis in a given case[[1]](#footnote-1) (and it may not be safe to assume that for a category of requests that the balance of interests is always in favor of disclosure; certain cases, such as investigations or prosecutions that could lead to capital punishment, might be especially problematic); and (iv) assurances that improper data types or volumes will not be disclosed to requesters (e.g., rule-based monitoring or blocking of unusual request sizes, permissioning systems). (3.9 – 3.12)
	+ Individual rights: address how data subject requests are handled, including (i) access rights to request logs (which may themselves be high risk or even "special category" personal data); (ii) appropriate time period for retention of those logs; (iii) the manner in which information is provided to data subjects; (iv) how to deal with situations where Requestor insists on not providing information to the data subject (e.g., law enforcement confidentiality); and (v) requests to restrict or block processing. (3.13 – 3.16)
	+ Data transfer: for international data transfers, EPDP envisages relying on the EU Standard Contractual Clauses (SCC) legal safeguarding mechanism, however (i) some Requestors, including public authorities, will not agree to their terms; (ii) the terms of the SCCs are not easy to comply with, especially at scale; (iii) if EEA Contracted Parties are processors they cannot directly rely on SCCs to transfer data to ICANN org or Requestors outside of the EEA, so a workaround would need to be found. (3.17)
	+ Security: safeguards should be proportionate to the risk to data subjects should their data be compromised. (3.18)

**3. What is the Risk of Liability to Contracted Parties for Disclosure?**

* If the safeguards are inadequate or abused/circumvented by Requestors (or other aspects of the GDPR are contravened, e.g. inadequate notice or lack of a legal basis for processing), Contracted Parties could face investigations, enforcement orders (e.g. processing prohibitions), and (financially) both liability to individuals (civil) and liability to supervisory authorities (fines).
* In broad strokes, B&B offers in pertinent parts that (1) where parties are joint controllers, this does not mean that the parties each have to undertake all elements of compliance, (2) if CPs are processors, they will only be liable to individuals (civil liability) 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, (3) even when parties are deemed to be joint controllers, recent court decisions (concerning enforcement by supervisory authorities) have emphasized that joint control does not imply equal responsibility for breaches of the GDPR, and (4) CPs, as joint controllers with ICANN org, would benefit from clear allocation of responsibilities under the terms of the joint controllership “arrangement” they must enter into pursuant to GDPR Art. 26.

*Liability to individuals*

* GDPR Article 82 sets out the rules on liability to individuals. (4.2)
* Controllers are liable for damages caused by processing that violates GDPR. Processors are liable for damages caused by processing where the processor has not complied with processor specific requirements or where the processor acted outside of or contrary to instructions from the controller. (4.2)
* A controller or processor is not liable if it proves it was in no way responsible for the event resulting in damages. (4.2)
* Where multiple controllers or processors involved in the same processing, each entity is liable for the entire damages (joint and several liability) to individuals (4.2, 4.3)
* If Contracted Parties are processors, they are only liable if they fail to comply with processor-specific obligations under GDPR or act outside or contrary to instructions from the controller. In such a scenario, it is unlikely Contracted Parties would violate the controller’s instructions because the SSAD is automated; the more likely source of liability for them, therefore, would be for having inadequate security measures, or failing to comply with the GD{PR's rules on international data transfers. Contracted Parties could look to ICANN org to prescribe security and international transfer arrangements to give Contracted Parties ability to argue that they are “not in any way responsible for the event giving rise to the damage.” (4.4)
* If Contracted Parties are controllers, and if disclosure violates GDPR, they are unlikely to avoid liability to individuals if they cannot prove that they are “not in any way responsible for the event giving rise to the damage,” if they actively participate in the disclosure event.
* Any liability creates the potential that Contracted Parties would be liable for all damages to the data subject. This risk is highest under a joint controller scenario. (4.5, 4.6).
* Contracted Parties held liable for the entirety of damages to a data subject can seek appropriate contributions from other responsible parties. (4.7)
* As controllers, Contracted Parties and ICANN would have a positive obligation to address the risk of Requestors seeking improper access to personal data. Safeguards must be appropriate to the level of risk. If a Requestor circumvents SSAD safeguards, courts might accept that the safeguards were adequate, which would limit Contracted Parties' primary liability. (4.9, 4.10)
* Even in the event of a GDPR breach caused by a Requestor, the Contracted Parties, ICANN, and the Requestor may be deemed “involved in the same processing” with each party jointly and severally liable for damages arising from that breach. Contracted Parties and ICANN may be able to argue that they are “not in any way responsible for the event giving rise to damage” but otherwise would need to seek recovery from the Requestor or join the Requestor in the initial proceedings in order to apportion damages. (4.11)

*Liability to supervisory authorities*

* Supervisory authorities may proceed against controllers or processors. (4.12)
* It is unclear whether joint and several liability applies where multiple parties are involved in processing (i.e., enforcement action arguably isn’t appropriate if others are responsible). (4.13)
* There needs to be clear wording in a law, to impose joint and several liability - this strengthens the argument that this would have been stated expressly if it was intended in respect of fines from supervisory authorities. Art. 83(2)(d) makes it clear that joint/several liability doesn’t apply concerning supervisory authorities. (4.13.2)
* Even when parties are joint controllers, recent court decisions (about enforcement by supervisory authorities) emphasize that joint control doesn’t imply equal responsibility for GDPR breaches. (4.13.4)
* Contracted Parties and ICANN would therefore benefit from clearly allocated responsibilities under a joint controllership arrangement (and a joint controllership arrangement is in any case mandatory, in all joint control siutations, pursuant to GDPR Art. 26). (4.14)
* It may be possible to take advantage of the “lead authority” (a.k.a. "one stop shop" or "consistency") provisions of GDPR to ensure that any enforcement action takes place through ICANN org’s Brussels establishment, rather than against Contracted Parties. This mechanism is only available where there is cross-border processing of personal data (entities in multiple EEA member states, or effects on data subjects in multiple EEA member states). (4.15 – 4.17)
* The “lead authority” provisions in GDPR don’t specifically address joint controllerships, but guidance suggests that if ICANN org and Contracted Parties designated ICANN’s Belgian establishment as the main establishment for the processing (i.e., where decisions regarding processing are made) it may minimize the risk of enforcement directly against Contracted Parties. This is a novel and untested approach. (4.15 – 4.20)

Annex:

Legal Questions 1 & 2: Liability, Safeguards, Controller & Processor

As the EPDP Team deliberated on the architecture of an SSAD, several questions came up with respect to liability and safeguards. In response, the Phase 2 Legal Committee formulated the following questions to outside counsel:

1. Consider a System for Standardized Access/Disclosure where:

o contracted parties “CPs” are contractually required by ICANN to disclose registration data including personal data,

o data must be disclosed over RDAP to requestors either directly or through an intermediary request accreditation/authorization body,

o the accreditation is carried out by third party commissioned by ICANN without CP involvement,

o disclosure takes place in an automated fashion without any manual intervention,

o data subjects are being duly informed according to ICANN’s contractual requirements of the purposes for which, and types of entities by which, personal data may be processed. CP’s contract with ICANN also requires CP to notify data subject 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. CP has done so.

Further, assume the following safeguards are in place

* ICANN or its designee has validated/verified the requestor’s identity, and required in each instance that the requestor:
	+ represents that it has a lawful basis for requesting and processing the data,
	+ provides its lawful basis,
	+ represents that it is requesting only the data necessary for its purpose,
	+ agrees to process the data in accordance with GDPR, and
	+ agrees to EU standard contractual clauses for the data transfer.
* ICANN or its designee logs requests for non-public registration data, regularly audits these logs, takes compliance action against suspected abuse, and makes these logs available upon request by the data subject.

a. 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?

b. Would you deem the criteria and safeguards outlined above sufficient to make disclosure of registration data compliant? If any risk exists, what improved or additional safeguards would eliminate[[2]](#footnote-2)1 this risk?

c. In this scenario, would the CP be a controller or a processor[[3]](#footnote-3)2, and to what extent, if at all, is the CP’s liability impacted by this controller/processor distinction?

d. Only answer if a risk still exists for the CP: 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 (misdemeanor or felony) or the associated sanctions (fine, imprisonment or capital punishment)?

2. To what extent, if any, are contracted parties liable when a third party that accesses non-public WHOIS data under an accreditation scheme where by the accessor is accredited for the stated purpose, commits to certain reasonable safeguards similar to a code of conduct regarding use of the data, but misrepresents their intended purposes for processing such data, and subsequently processes it in a manner inconsistent with the stated purpose. Under such circumstances, if there is possibility of liability to contracted parties, are there steps that can be taken to mitigate or reduce the risk of liability to the contracted parties?

1. If disclosure is a legal obligation pursuant to EU or EU/EEA Member State laws (including treaties to which the EU or a relevant member State is a party), there is no need to consider the legitimate interests test. [↑](#footnote-ref-1)
2. “Here it is important to highlight the special role that safeguards may play in reducing the undue impact on the data subjects, and thereby changing the balance of rights and interests to the extent that the data controller’s legitimate interests will not be overridden.“ [https://iapp.org/media/pdf/resource\_center/wp217\_legitimate-interests\_04-2014.pdf](https://urldefense.proofpoint.com/v2/url?u=https-3A__iapp.org_media_pdf_resource-5Fcenter_wp217-5Flegitimate-2Dinterests-5F04-2D2014.pdf&d=DwMGaQ&c=FmY1u3PJp6wrcrwll3mSVzgfkbPSS6sJms7xcl4I5cM&r=8K75qGdDlOta4kh6k2F0jrT195M3tF3J_Fxcz6EvuG2kYKDeA67ZTEnthHXAPVXH&m=WmQKTNAW4Y5U-c0lyA5XiCXNYR3bBOIeUD3JHAistCY&s=sWyYss17bzERUGYmyRgrLIYOWeEFfEm8TK82oD0K4Yg&e=) [↑](#footnote-ref-2)
3. [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor\_en](https://urldefense.proofpoint.com/v2/url?u=https-3A__ec.europa.eu_info_law_law-2Dtopic_data-2Dprotection_reform_rules-2Dbusiness-2Dand-2Dorganisations_obligations_controller-2Dprocessor_what-2Ddata-2Dcontroller-2Dor-2Ddata-2Dprocessor-5Fen&d=DwMGaQ&c=FmY1u3PJp6wrcrwll3mSVzgfkbPSS6sJms7xcl4I5cM&r=8K75qGdDlOta4kh6k2F0jrT195M3tF3J_Fxcz6EvuG2kYKDeA67ZTEnthHXAPVXH&m=WmQKTNAW4Y5U-c0lyA5XiCXNYR3bBOIeUD3JHAistCY&s=VLfFI2qvdMLP-znynFRMTpavBVBxa6oxjPohOdyWao0&e=) [↑](#footnote-ref-3)