**ICANN org Comments on 7 November 2018 Memo From Thomas Rickert regarding Processors, Controllers, Co-Controllers and Joint Controllers**

15 November 2018

As requested by the EPDP Team for ICANN org to contribute to the discussion on roles and responsibilities, this document provides ICANN org’s comments to the 7 November 2018 memo titled “Processors, Controllers, Co- Controllers, and Joint Controllers” as prepared by Thomas Rickert (with edits from Diane Plaut) (the “[Roles and Responsibilities Memo](https://community.icann.org/download/attachments/97846713/Input%20EPDP%20on%20responsibilities%20wdp%20edits.pdf?version=1&modificationDate=1541775903000&api=v2)”). This document is not an official ICANN org or Board position but is intended to provide additional input from ICANN org into the ongoing deliberations of the EPDP Team about whether or not Article 26 of the European Union’s General Data Protection Regulation (GDPR) applies to processing activities concerning gTLD registration data. The possible status of ICANN and the contracted parties as joint controllers is not a matter of the preferences of the parties, but it is ultimately a question of law about whether Article 26 of the GDPR applies. This legal question requires further analysis and discussion.

1. Key Roles established by the gdpr
	1. Controller: Under the GDPR, “controller” means 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. Processor: A “processor”, on the other hand, designates the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
	3. Joint Controllers:The GDPR expressly contemplates that there can bejoint controllers of personal data with regard to a particular processing activity. This occurs when there are two or more controllers jointly determining the purposes and means of the processing.[[1]](#footnote-2) In other words, joint controllers together decide whether, for what reason (“the why”), to what extent, and the material technical means and methods (“the how”) of the data processing.
		1. Joint controllers do not necessarily have to equally share the determination of the processing. Joint controllers can share all means and purposes of a processing or a portion of the means of processing.[[2]](#footnote-3)
		2. Joint controllers are effectively jointly and severally liable for compliance with the GDPR, which may have far-reaching consequences for every party in a joint controllership scenario.
	4. Independent Controllers: As another alternative, there also could be multiple independent controllers for the same personal data set. This occurs when each controller independently determines the purpose or means of processing for the same data. Just because multiple controllers may be involved in a processing activity does not automatically mean they are joint controllers. Indeed, they could be independent controllers for the same personal data set.
		1. The Article 29 Working Party (WP29) issued guidance on this concept.[[3]](#footnote-4) The WP29 recognized that “the mere fact that different subjects cooperate in processing personal data, for example in a chain, does not entail that they are joint controllers in all cases, since an exchange of data between two parties without sharing purposes or means in a common set of operations should be considered only as a transfer of data between separate controllers.” [[4]](#footnote-5)
		2. For example, a travel agency sends personal data of its customers to the airlines and a chain of hotels, with a view to making reservations for a travel package. The airline and the hotel confirm the availability of the seats and rooms requested. The travel agency issues the travel documents and vouchers for its customers. In this case, the travel agency, the airline and the hotel will be three different data controllers, each subject to the data protection obligations relating to its own processing of personal data.

This example illustrates that multiple controllers are independent from each other and use the same data set for different purposes. Where there are multiple controllers, no agreement is required; both controllers have their own responsibility under GDPR for their own processing activities.

1. Previous guidance regarding roles of icann, registries, and registrars
	1. The question of whether ICANN and contracted parties are some type of controller or processor with respect to various processing activities has been discussed in various analyses leading up to the adoption of the Temporary Specification for gTLD Registration Data (the “Temporary Specification”). For example, the WP29 offered a preliminary reaction on the question in its 6 December 2017 letter to ICANN. The WP29 noted: “At first glance it would seem that since ICANN and the registries jointly determine the purposes and means of the processing of personal data for the WHOIS directories, ICANN and the registries are joint controllers. This would mean that both ICANN and the registries must ensure that personal data are processed in accordance with the obligations of the European data protection laws.”[[5]](#footnote-6)
	2. The Hamilton law firm offered the following analysis in its 16 October 2017 memorandum[[6]](#footnote-7):

*With regard to the personal data processing carried out in relation to the Whois services, different parties can be the controller for different processing purposes. For instance, ICANN is for sure to be considered as the controller in the context that it requires registrars and registries to obtain certain data and, through its agreements and policies, directs the processing of data within the scope of the Whois services. However, we understand that registrars and registries may control certain parts of the processing on their own, for instance where a registrar chooses to obtain additional personal data, which could make them the controller with regard to certain processing.*

*While it in theory might be possible to determine which party of ICANN, a registrar and a registry is the controller of any given processing of personal data within the framework of the Whois services, this will most likely be a difficult exercise in practice, as the parties have different influence over different parts of the processing. In light hereof, our recommendation would be to take the general approach that the involved parties are all considered to be joint controllers. This view would help mitigate the risk that a DPA makes a different assessment but would also offer a practical solution to the issue.*

* 1. Taking into account the initial input from the WP29 and part 1 of the Hamilton memo, ICANN org held further discussions with the community (including contracted parties) to more specifically identify the flow of gTLD registration data to better understand whether or not Article 26 of the GDPR applies. Based on this work, ICANN org’s 8 March 2018 publication titled “Interim Model for Compliance with ICANN Agreements and Policies in Relation to the European Union’s General Data Protection Regulation (the “Cookbook”) takes the position that, “ICANN has determined that each contracting party is acting as an independent controller in connection with the processing of WHOIS data.”[[7]](#footnote-8) This understanding of Article 26 of the GDPR is also reflected in the Temporary Specification, which identifies where ICANN, Registries, and Registrars act as controllers with respect to specific gTLD processing activities but does not indicate that any of the parties are joint controllers with each other.
	2. ICANN org’s position in the Cookbook and Temporary Specification takes a different approach from the Hamilton memo for the same reasons it raises questions with the Roles and Responsibilities Memo. Additional analysis of the parties’ responsibilities with respect to the processing must be completed, even if this is a difficult task. Without such an analysis, a joint controllership that generally covers all processing could lead to lack of transparency and lack or guidance/direction regarding what each contracted party is responsible for. Additionally, the Article 29 Working Party’s comments “at first glance” are not binding and underscore that a more careful assessment is required.
1. Position in the Roles and Responsibilities Memo concerning the roles of icann, registries, and registrars
	1. The Roles and Responsibilities Memo states that ICANN, Registrars and Registries are Joint Controllers for “the set of operations of domain registration”. The Roles and Responsibilities Memo seems to take the legal interpretation that “[…] Jointly must [be] interpreted “as meaning ‘together with’ or ‘not alone’ in different forms and combinations” and the assessment of joint control should mirror the assessment of ‘single’ control*.*”[[8]](#footnote-9)
	2. According to this view, “it cannot be assumed that ICANN and the contracted parties are co-controllers for the processing of data, rather than joint controllers.” The Roles and Responsibilities Memo adds that “a co-controllership would require two or more parties which are completely independent of one another, co-operatively working together in the processing of data but for different purposes.”[[9]](#footnote-10)
2. Key questions for further discussion

The following sets out key points to add to the discussion on the Roles and Responsibilities Memo. These points provide additional viewpoints to help assess whether or not Article 26 of the GDPR applies to various gTLD registration data processing activities. The points are not intended to be exhaustive; other issues may arise and should be further discussed among the EPDP Team, and ICANN org looks forward to participating in further discussions.

Overall, ICANN org agrees that it is important to understand the roles and responsibilities of the contracted parties with regard to the relevant processing activities. It is only by doing so that the parties can clearly assess when they are controllers, and, in turn, independent or joint controllers and the applicability of Article 26 of the GDPR.

* 1. **It Is Important to Determine ICANN’s and Contracted Parties’ Responsibilities for Any Processing Activities**
		1. The Roles and Responsibilities Memo states that “the processing of registration data is covered by the overarching purpose of the registration of a domain name by all three parties in this process.” Also, it notes that, “processing should not be artificially divided into smaller processing steps, but can be uniformly considered as a set of operations. In this respect, data collection, passing on to the registry, review and implementation and ongoing management of the registration can be considered as one set of ‘domain registration’ operations, because it pursues the overall purpose of registering the domain for a new registrant.” It would be helpful to understand this analysis in the context of the approach currently being undertaken by the EPDP Team – to carefully assess each party’s roles with respect to each processing activity. The current EPDP Team’s approach to assess each processing activity and the related roles and responsibilities seems to be what is needed for a proper assessment of the applicability of Article 26 of the GDPR so that the parties are not relying on assumptions to reach conclusions that may in turn carry heavy consequences from a liability perspective. The approach of differentiating processing activities may also increase transparency for data subjects about how their data is being processed.
		2. Additionally, not undertaking the exercise of delineating processing activities among the contracted parties may be seen to be in contradiction with the approach by the supervisory authorities in the EU and how they have historically reviewed cases (see for example the so-called SWIFT case[[10]](#footnote-11) in 2006 in which the authorities assessed each processing activity separately). It may be possible that ICANN and the contracted parties, if at all, are joint controllers for certain, limited, and clearly defined processing activities, but not for “any and all” such activities.
		3. There are several good reasons to differentiate processing activities amongst the parties:
			1. There are no joint purposes “across the board” where the various parties in the domain name ecosystem (e.g. ICANN, contracted parties, data escrow providers, etc.) act as joint controllers. There only needs to be a joint controllership arrangement in limited cases – if any – where the parties jointly determine the purposes and the means. It would be helpful to the analysis of how Article 26 might apply if the EPDP Team could walk through specific examples of processing activities to determine whether or not certain activities are or are not fully “joint” activities of all of the parties.[[11]](#footnote-12)
			2. Determining the processing activities ensures the respective responsibilities are clearly defined and understood. This is essential since, as mentioned above, not all (if any) processing activities are carried on by the contracted parties as joint controllers.
			3. The Roles and Responsibilities Memo provides that the goal of the GDPR is to “primarily protect of the rights and freedoms of data subjects. This document is intended to address the clear allocation of responsibilities in relation to ensure the rights of data subjects.”[[12]](#footnote-13) However, if the proposal in the Roles and Responsibilities Memo not to single out processing activities is taken, it is not clear how this approach would promote transparency since all contracted parties would be a party and it would prove difficult to demonstrate who is responsible for what. It would seem that data subjects would not know who is responsible for the processing of their personal data and the protection of their rights, which ultimately will be detrimental to them.
			4. As noted in the Roles and Responsibilities Memo, “[t]he factual control of the data processing, as well as control over external effects vis-à-vis the data subject, is determinative when reviewing responsibility.”[[13]](#footnote-14) As part of the discussion about factual control over data processing activities, how should processing by Registries, ICANN, Data Escrow Providers, Dispute Resolution Providers, etc. be factored into the analysis since these parties have no direct contractual relationship with the data subjects and data may only be available to them in limited circumstances?
	2. **Future EPDP Team Discussions Also Should Focus on the Means of Processing**
		1. The Roles and Responsibilities Memo does not seem to differentiate purposes and means of processing.
			1. The Roles and Responsibilities Memo states: “[…] it must be *assumed* that ICANN, registrars and registries jointly determine the purposes and means of processing that are compulsory for domain registration overall. In this respect, these are responsible for this set of operations pursuant to Art. 4 no. (7) and 26 GDPR.”[[14]](#footnote-15) (emphasis added)
			2. The Roles and Responsibilities Memo further provides that because “ICANN specifies a purpose for the processing operation overall”, it *must* be a joint controller.
		2. To qualify as a controller, an entity must be capable of determining the “purpose” and the “means” of the processing. When using “purpose” and “means” to assess whether or not an entity is a controller, a crucial factor is in the level of influence on the “why” and “how” of processing activities. A controller has discretion to determine the purposes of the processing and has greater latitude in making decisions with respect to the data. Determining the “means” of processing includes both technical and organizational questions where some decision-making power can be delegated to processors.

The EPDP Team has spent time discussing purposes of processing, but it does not seem that there has been an opportunity to focus attention on the means of processing. Both components should be equally analyzed to assess where there is controllership or joint controllership. The purposes and means need to be treated separately, to determine the extent to which each party determines the purposes and the means of the processing. This analysis will help factor into the overall goal of understanding whether or not as a matter of law the parties are controllers or joint controllers.

* 1. **A Joint Controller Arrangement Is not the Same as a Data Processing Agreement**
		1. A joint controllership arrangement for the relevant parties in the domain name ecosystem will be complex and may, to some extent also carry the risk of not being transparent. There is no “one size fits all” solution to this and the interests of the various stakeholders may lead to challenges that may not be easy to overcome. ICANN org has provided some implementation questions in Section 5 of this document to help begin the conversation on these points.
		2. A joint controllership arrangement is not comparable to a simple, more or less standardized data processing agreement pursuant to Art. 28 of the GDPR in terms of its nature and character. While Art. 28 GDPR clearly allocates what provisions must be included in a data processing agreement, there is no comparable or similar standard format for a joint controller arrangement available.
		3. The Temporary Specification presumes parties working as independent controllers, and details what the parties’ obligations are as independent controllers, consistent with the GDPR.
		4. If there is a joint controllership, there must be a careful assessment of the relevant data protection obligations, an appropriate assignment of these between the parties, and a common understanding and agreement on such assignment.
		5. The EPDP Team should also be aware that the “essential” provisions of the arrangement must be provided to the data subjects (i.e., Registrants).
		6. A joint controllership approach means also very extensive negotiations amongst the parties due to the consequences in terms of liability or other violations or deficiencies of duties.
	2. **Practical Questions For Structuring the Joint Controllership Arrangement**
		1. The EPDP Team, including contracted parties, should consider the form and the structure of a joint controller arrangement.
		2. Consider: Would the contacted parties need to have a single joint controller arrangement between ICANN org and all Registries and Registrars? Or would ICANN org have separate joint controller arrangements with each of the 2,500 + Registries and Registrars? Would every Registry be a joint controller with every Registrar, even if they don’t do business together? Would resellers be part of the joint controller arrangement? Back-end providers? Data escrow providers? Proxy registration services? Dispute resolution service providers? Zone file users? The Trademark Clearinghouse?
		3. Would there be one form of joint controller agreement to which all parties would execute, or would there be separate negotiations between ICANN and each of the 2,500+ contracted parties (or resellers or back-end providers)? (Would it still be a joint controller agreement if there are separate agreements between all of the relevant parties processing gTLD registration data?) What if one or more contracted parties disagree that they are joint controllers? What about contracted parties who primarily do business in jurisdictions outside of the European Economic Area; would they also be required to execute a (or "the"?) joint controller agreement?
	3. **Indemnification/Liability**
		1. If there is joint controllership, ICANN org agrees that it is customary and appropriate to address the allocation of protection obligations and GDPR compliance responsibilities, and the allocation of indemnification and liability protection in the joint controller arrangement.
		2. However, indemnification obligations should attach to defined data processing activities and responsibilities allocated to the joint controllers either as a matter of law under the GDPR or by agreement of the parties to ensure compliance, which vary depending on the nature of the processing.
		3. Indemnification should be mutual. Discussions so far seem to suggest a policy or agreement that would require ICANN alone to indemnify the Registries and Registrars. This approach is commercially not feasible and also undermines the nature of the collaborative approach taken to develop the policies and agreements that govern the ICANN community. All contracted parties are stakeholders in the policies that govern them; any indemnification should, by extension, reflect that relationship.
		4. A unilateral indemnification provision would further require a reassessment of the current financial arrangements. Application fees and other fees paid by Registrars (and their Registrants) may have to be increased to realize the higher liability costs. Another approach that could be explored might be shared contributions to a bond or insurance policy to cover this risk.
1. practical Scenarios for joint controllership – Questions for implementation

If the EPDP Team moves toward recommending a joint controllership arrangement, the parties should have a clear sense of what that relationship would mean in practice. Consider the following scenarios:

* + 1. The Roles and Responsibilities Memo provides that “[e]ven with a clear distribution of the responsibility between the controllers, all controllers are liable vis-à-vis external parties for the overall processing operation.”[[15]](#footnote-16) In a joint controllership, if there is a data breach caused by a Registrar located in India that impacts 10,000 of its Registrants, would ICANN and all registries and registrars then be liable? (Even registrars that don't do business with that registrar?) Or would there be a separate joint controller agreement for the registry and the authorized registrars for each TLD? (Does it follow that each ccTLD registry and its registrars would also be joint controllers if it is true that ICANN and gTLD registries and registrars are joint controllers? The EPDP team might want to identify and review any such joint controller agreements?)
		2. Who would be responsible for issuing notices to Registrants as the data subjects? What would happen if a notice is deficient? Would all parties be liable?
		3. Who would handle responding to data subjects rights? In a joint controllership, if a Registrar does not timely respond to one of its contracted Registrants, would all parties be liable?
		4. What would happen if a Belgian Registrar neglects to enter into EU Standard Contractual Clauses with a Data Escrow Agent located outside of the EU? Would all parties now liable?
		5. How would parties handle their respective relationships with other third parties such as Data Escrow Agents?

\*\*\*\*\*\*\*

ICANN org would like to thank the EPDP Team for the opportunity to provide comments on the Roles and Responsibilities Memo. We hope the additional input contained in this document is useful and look forward to further discussion of these issues in the coming weeks.

1. *See* Art. 26 (1) GDPR. [↑](#footnote-ref-2)
2. *See* p. 29 Opinion 1/2010 on the concepts of “controller” and “processor” (WP 169). [↑](#footnote-ref-3)
3. *See* Opinion 1/2010 on the concepts of “controller” and “processor”. Although the guidance was issued in the context of the EU Data Protection Directive and prior to the GDPR taking effect, it is to be considered still valid under the GDPR as the definitions of “controller” under the GDPR remain the same as its predecessor. [↑](#footnote-ref-4)
4. *See* id. at 19. [↑](#footnote-ref-5)
5. <https://www.icann.org/en/system/files/correspondence/falque-pierrotin-to-chalaby-marby-06Dec17-en.pdf> [↑](#footnote-ref-6)
6. See paragraphs 3.7.3 and 3.7.3 at <https://www.icann.org/en/system/files/files/gdpr-memorandum-part1-16oct17-en.pdf> [↑](#footnote-ref-7)
7. See paragraph 7.2.11.3 at <https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf>. [↑](#footnote-ref-8)
8. *See* p. 2 of the Roles and Responsibilities Memo. [↑](#footnote-ref-9)
9. *Id.* [↑](#footnote-ref-10)
10. See Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP128), *available at* <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf>) [↑](#footnote-ref-11)
11. ICANN org has questions about the position in the Roles and Responsibilities Memo that ICANN’s role in developing and drafting policies for the Contracted Parties makes it a controller (or joint controller). Although ICANN is not a governmental or regulatory body, by the logic in the Roles and Responsibilities Memo, it would seem that legislators or judicial bodies also are controllers by virtue of the fact that they develop and/or interpret regulations or guidelines for which organizations/persons must comply. Likewise, would all non-governmental policy or standard-setting bodies become controllers of the data by virtue of the fact that they set requirements or guidelines for their members? [↑](#footnote-ref-12)
12. *See* p. 2 of the Roles and Responsibilities Memo. [↑](#footnote-ref-13)
13. *See* p. 3 of the Roles and Responsibilities Memo. [↑](#footnote-ref-14)
14. *Id.* at 3. [↑](#footnote-ref-15)
15. *See* p 4. Roles and Responsibilities Memo. [↑](#footnote-ref-16)