The text below is from line 1694 to line 1934 on pages 37 through 43 in the Draft EPDP Final Report.

**Processors, Controllers, Co-Controllers and Joint Controllers**

Controller is the person or entity, that alone or jointly with others, determines the purpose and means of processing. Processing, in turn is “*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.*

Pursuant to Art. 4 no. (7) 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

In situations where two or more controllers “jointly” determine the purposes and means of processing, Art. 26 GDPR specifies additional requirements that apply (“Joint Controller”).

In contrast to controllers, processors do not have the right to make decisions with regard to the purposes and means of processing, but act for the contractor (controller) with a duty to comply with the controller(s)’ instructions.

Processors can be afforded some discretion in deciding on the means of processor, whereas a determination of the purposes of processing is usually a function reserved to controllers.[[1]](#footnote-2)

The purpose of processing is an “expected result that is intended or guides planned actions”. The means of processing is the “type and manner in which a result or objective is achieved”[[2]](#footnote-3).

Processors are distinguished from controllers based on the following criteria:

* A person or entity that has no legal or factual influence on the decision concerning the purposes for and manner in which personal data is processed cannot be a controller.
* A person or entity that alone or jointly with others decides on the purposes of processing is always a controller.
* The controller may also delegate the decision(s) concerning the means of processing to the processor, but the controller cannot delegate the “essential elements which 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?’ ‘who shall have access to them?’, and so on.”
* Processors are independent legal persons who are different from the controller and who process data on behalf of the controller(s) without deciding on the purposes of processing.[[3]](#footnote-4)

Where two or more different organizations jointly determine the purposes or the essential elements of the means of the processing they will be joint controllers and must enter into an arrangement as required by Art. 26 of the GDPR. The participation of the parties to the joint determination may take different forms and does not need to be equally shared. Jointly must 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”.

ICANN and the EPDP Charter Questions and How the Above Principles are Applied Herein

As discussed below, 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.

Purpose of Art. 26 GDPR

The regulation is to primarily protect of the rights and freedoms of data subjects.[[4]](#footnote-5) This document is intended to address the clear allocation of responsibilities in relation to ensure the rights of data subjects. In more complex role allocations, e.g. in the area of domain registration with several distribution levels, the data subject’s right of access and other rights are to be guaranteed across levels.[[5]](#footnote-6)

“The definition of the term “processing” listed in Article 2 lit. b of the guideline does not exclude the option that diverse actors participate in diverse operations or sets of operations in connection with personal data. These operations can be executed simultaneously or in diverse stages. In such a complex environment it is even more important that roles and responsibilities are allocated to ensure that the complexity of joint control does not result in an impractical division of responsibility that would affect the effectiveness of data protection law.”[[6]](#footnote-7)

Recital 79 GDPR furthermore clarifies that the regulation is to simplify monitoring by the supervisory authorities.

The factual control of the data processing, as well as control over external effects vis-à-vis the data subject, is determinative when reviewing responsibility.

Furthermore, 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. This also applies if diverse agencies pursue different purposes within the processing chain, when engaged in the detail of smaller processing steps on a micro level. On a macro level, the same purpose is pursued overall with all small steps in the chain, so that a uniform set of operations specifically applies here (Art.29 Group WP 169, p. 25).

Differentiation is required when considering the operation of collecting and processing the data collected by the registrar from its customers in order to create an invoice, to maintain a customer account, and to manage the contractual relationship with its customers. This data fulfils another purpose that is not codetermined by the registry and ICANN.

Further analysis should be carried out to determine, for the table below, which processing activities are determined jointly and which are not.

This also corresponds to the legislative intent to have clear and simple regulations concerning responsibility in case of multiple participants and complex processing structures, and to prevent a splitting of responsibilities to protect the data subjects as far as possible.

Pursuant to Article 1 Section 1.1 of the ICANN bylaws, ICANN has responsibility:

*“to ensure the stable and secure operation of the Internet's unique identifier systems as described in this Section 1.1(a) (the "****Mission****"). Specifically, ICANN:*

*(i) Coordinates the allocation and assignment of names in the root zone of the Domain Name System ("****DNS****") and coordinates the development and implementation of policies concerning the registration of second-level domain names in generic top-level domains ("****gTLDs****"). In this role, ICANN's scope is to coordinate the development and implementation of policies:*

· *For which uniform or coordinated resolution is reasonably necessary to facilitate the openness, interoperability, resilience, security and/or stability of the DNS including, with respect to gTLD registrars and registries, policies in the areas described in Annex G-1 and Annex G-2;”*

As already stated, ICANN fulfils this responsibility among other things by contractually specifying for the various participants the data which must mandatorily be collected and retained.

Joint and several liability

Irrespective of joint control, if two or more controllers are involved in the “same” processing then there will be joint and several liability unless a party can provide it is not responsible for the event giving rise to the damage (Art. 82). The factual responsibility may be adjusted only *inter parties*. Therefore, having clear allocations between the parties is even more important *inter parties*.

Fines

However, such joint and multiple liability may not apply to fines under Art. 83 (4) lit. a) GDPR. In this respect, registry and registrar are liable pursuant to their role allocation for breaches in their area or against duties under the GDPR, which were incumbent upon them within the scope of the contractual basis.

Joint Controller Arrangement

Joint controllers must furthermore specify, in a transparent form, who fulfills which duties vis-à-vis the data subjects, as well as who the contact point for data subject’s rights is (Art. 26 (1) p. 2 GDPR).

However, the data subject is authorized to address any of the participating responsible agencies to assert its rights, regardless of the specification concerning competence (Art. 26 (3) GDPR).

The arrangement is to regulate the specific controllers that are to fulfill the duties prescribed by GDPR. Pursuant to Recital 79 GDPR, the following must be specifically regulated in a transparent form:

* + how the relations and functions of the controllers among each other are designed, and
	+ how roles are distributed between controllers to fulfill data subject rights of registrants.

Article 26 permits the parties to allocate responsibility for providing notice to the party best able to fulfill the obligation However, Art. 26 GDPR suggests that multiple controllers fulfill information obligations centrally. Details shall be agreed upon between the parties.

Therefore, in relation to the above, as described, the EPDP, has set forth within the Initial Report, the Responsibility of each named party in relation to the specified Purposes, listed and based on the legal basis recommendations, for the respective Purpose and in relation to its duties performed for the data subject.

In relation to Preliminary Recommendation #13 below, the EPDP Team understands that relationship between ICANN Org, Registries and Registrars requires work at a greater level of granularity than in this report. During the further work of the EPDP and negotiations that will subsequently take place between the Registries, Registrars and ICANN in relation to memorializing the relationships between the parties for various processing activities the parties shall conduct a detailed review of the individual processing activities and the actions to be taken by the respective parties to determine if there is joint control and the scope of any joint control; and b) (irrespective of joint control) to allocate responsibility. If there is joint control, then any arrangement shall meet the requirements of Art. 26 sec 2 of the GDPR (including a document being made to data subjects), which specifies:

"The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject."

A clear demarcation the processing activities covered by the arrangement versus those carried out by either party outside the scope of the arrangement shall be documented.

The arrangement shall recognize that parties are currently using third parties’ services or otherwise work with third parties, such as

* Data Escrow Agents
* EBEROs
* Registry Service Providers
* Registrar as a Service Providers
* Resellers
* Dispute Resolution Providers
* the TMCH.

This may or may not include processing of personal data by those third parties. Where personal data is processed by third parties, the respective arrangement will need to ensure that the data processing is carried out in a way compliant with GDPR. However, conditional to GDPR compliance, nothing in the arrangement shall prevent the respective parties from engaging third parties and entering into the required agreements without further authorizations from the other parties.

1. *Klabunde*in *Ehmann/Selmayr*„Datenschutz-Grundverordnung“ Art.4 marg. no. 29 [↑](#footnote-ref-2)
2. Art. 29 Data Protection Working Party, Statement 1/2010 of 16 February 2010, p. 16, available at <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf> [↑](#footnote-ref-3)
3. Art. 29 Data Protection Working Party, Statement 1/2010 of 16 February 2010, p. 18, 39, 40, available at <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf> [↑](#footnote-ref-4)
4. *Bertmann*in *Ehmann/Selmayr*“Datenschutz-Grundverordnung” Art. 26, marg. no. 1 [↑](#footnote-ref-5)
5. Art. 29 Data Protection Working Party, Statement 1/2010 of 16 February 2010, p. 27, available at <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf> [↑](#footnote-ref-6)
6. Art. 29 Data Protection Working Party, Statement 1/2010 of 16 February 2010, p. 22, available at <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf> [↑](#footnote-ref-7)