**ICANN org Response to Request from the EPDP Team for Additional Information re: Independent Controllers under the GDPR**

WORKING DRAFT FOR EPDP TEAM REVIEW AND DISCUSSION – 14 January 2019

As requested by the EPDP Team, this document provides additional information from ICANN org to help inform the ongoing deliberations of the EPDP Team about whether Article 26 of the European Union’s General Data Protection Regulation (“GDPR”) applies to processing activities concerning gTLD registration data. This document outlines an alternative approach to joint controllership for identifying the roles and responsibilities of the participants processing gTLD registration data. ICANN org continues to analyze the issue and this document does not present ICANN org’s or the ICANN Board’s final view of the matter; rather, based on analysis to-date, the document provides an alternative view for consideration by the EPDP Team to stimulate further discussion. The possible status of ICANN org and the contracted parties as joint controllers or independent 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.

1. introduction/summary overview

On November 21, 2018, the GNSO Expedited Policy Development Process (“EPDP”) Team on the Temporary Specifications for gTLD Registration Data issued an Initial Recommendations Report (“Initial Report”).[[1]](#footnote-2) In the Initial Report, the EPDP Team concluded that Registries, Registrars and ICANN org must be “assessed as joint controllers,” as defined under the GDPR “for the set of operations of domain registrations”.[[2]](#footnote-3) The Initial Report asserts that a “domain registration can mandatorily be performed only jointly by a Registrar and a Registry and governed by ICANN for gTLDs.”[[3]](#footnote-4) Thus, by extension “it must be assumed that ICANN, registrars and registries jointly determine the purposes and means of processing that are compulsory for domain registration overall” and are therefore responsible for this set of operations as joint controllers.[[4]](#footnote-5)

This document outlines why independent controllership with respect to gTLD registration data processing more broadly is a sound legal conclusion under the GDPR. The main reason for this is that the processing of gTLD registration data is not one set of “domain registration” operations as assumed in the Initial Report. From ICANN org’s perspective, gTLD registration data processing consists of various processing activities which occur under a common framework of agreements and policies. Under this framework, ICANN org and the contracted parties have separate and distinct purposes of processing, and each party exercises independent discretion on the means of such processing with respect to gTLD registration data. Therefore, the parties are independent and not joint controllers under the GDPR.

Additionally, as further explained below, independent controllership has advantages over joint controllership, including that it allows the parties to adopt a flexible data protection framework, which is easier to implement and maintain than a complex joint controllership arrangement. In contrast, joint controllership arrangements result in unwanted and unjustified liability risks stemming from joint and several liability among the parties, and create costly oversight, administration and reporting structures.

As a result, the EPDP Team can address the parties’ obligations under the GDPR in connection with gTLD data processing by maintaining independent controllership — preferably, by adopting a uniform data protection specification that would become part of each contract with a contracted party. While the GDPR does not require the adoption of such specification, as it contains no requirement for independent controllers to enter into any formal arrangement or written agreement, it could be beneficial for the parties to continue with the approach taken in Appendix C of the Temporary Specification and set out relevant independent controller obligations.[[5]](#footnote-6) Appendix C of the Temporary Specification could be further refined to serve as independent controller specification for ICANN org and the contracted parties. The refined Appendix C of the Temporary Specification could also serve in the future as the basis for a code of conduct pursuant to Art. 40 GDPR, which, as explained in Section IV.C.4\_below, would provide greater legal certainty for ICANN org and the contracted parties, as it would require authority approval and oversight by accredited bodies.

1. processing of Gtld registration datA as an independent controller activity
   1. Applicability of the GDPR

The GDPR governs the processing of personal data in gTLD registrations of residents of the European Economic Area (“EEA”) by EEA-based Registrars and Registries[[6]](#footnote-7) as well as the processing of EEA Registrants’ personal data targeted by non-EEA Registrars and Registries.[[7]](#footnote-8) Within the scope of the GDPR, Registries and Registrars process EEA personal data for various purposes in connection with the gTLD registration data, and are each subject to the provisions of the GDPR. As explained below, this document presents the reasoning as to why ICANN org and the contracted parties can be viewed as each independently operating as controllers.

* 1. Why it is Important to Distinguish Between “Controllers” and “Processors” under the GDPR

In light of the different roles and respective responsibilities of ICANN org and each contracted party under the GDPR, it is important for ICANN org and the contracted parties to identify (a) whether they are involved in the processing of personal data and (b) if so, whether they are operating as controllers or processors with respect to the specific processing of personal data in gTLD registrations. This is particularly important in situations where it will be necessary to determine which entity has data protection responsibility and can be held accountable with regard to certain compliance obligations, including obligations vis-à-vis the data subjects, as controllers and processors have different roles and responsibilities under the GDPR. This is why it is beneficial to establish the roles of the parties at the outset.

* 1. Controllership under the GDPR

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.
  + 1. Determining the Purposes and Means of Processing

To qualify as a controller, an entity must be able to determine the “purposes” and the “means” of the personal data processing. When using “purpose” and “means” to assess whether an entity is a controller, a crucial factor is in the level of influence (i.e., level of control) on the “why” and “how” of processing activities, as explained below.

* + - 1. *Purpose of the Processing*

The purpose of the processing is determining the “why” of the processing. A controller has discretion to determine the purposes of the processing and has greater latitude in making decisions with respect to the data.

The UK Supervisory Authority (“Information Commissioner’s Office”, “ICO”) has issued guidance on controllers. Although the ICO’s guidance dates back to 2014 and might lose some of its relevance for other EU data protection authorities as a result of Brexit, nevertheless, it is helpful as a practical guide to determine controllership. The guidance sets out questions that entities/persons should answer in their respective roles as controllers. Specifically, controllers decide:

* To collect the personal data in the first place and on the legal basis for doing so;
* Which items of personal data to collect (*i.e.*, the content of the data);
* Which data subjects to collect data about;
* Whether to disclose the data, and if so, to whom;
* Whether data subject access and other data subjects’ rights apply (*i.e.*, whether exemptions apply relieving a controller from the obligation to respond to data subject right requests); and
* How long to retain the data or whether to make non-routine amendments to the data.[[8]](#footnote-9)
  + - 1. *Means of the Processing*

In Opinion 1/2010 on the concepts of “controller“ and “processor” (WP169), the Art. 29 Working Party (“WP”) provided that determining the “means” of processing includes both, technical and organizational questions where decision-making power can be delegated to processors and “essential elements” 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?,” etc. [[9]](#footnote-10)

The ICO also has provided illustrative examples that data processors decide. These include:

* Which hardware or software shall be used;
* How to store the personal data;
* The security surrounding the personal data;
* The means used to transfer the personal data from one organization to another;
* The means used to retrieve personal data about certain individuals;
* The method for ensuring that a retention reschedule is adhered to;
* The means used to delete or dispose the data.[[10]](#footnote-11)

However, essential questions remain reserved for controllers to determine, such as “which data shall be processed?”, “for how long shall they be processed?”, “who shall have access to them?”[[11]](#footnote-12) Therefore, an entity that has decision-making authority about the storage period of personal data and on the access thereto will usually be qualified as controller, while such entity may delegate the decision on the means of processing to a processor, where only technical or organizational questions are concerned.[[12]](#footnote-13) Nevertheless, such decision-making power must entail an element of control and not just exist on a policy-making level (as discussed further below under Section ‎III.E)

* 1. What is a Processor?

Under the GDPR, a processor means:

* the natural or legal person, public authority, agency or other body
* which processes personal data on behalf of the controller.[[13]](#footnote-14)

There are two basic conditions to qualify as a processor:

* being a separate legal entity external to the controller, and
* processing personal data on the controller’s behalf.[[14]](#footnote-15)

The most important element is processing *on behalf of* *the controller*. Acting on behalf means serving in someone else’s interest, and in the context of data protection law, a processor acts in compliance with the instructions of the controller at least with respect to the purposes of the processing – whether the processing activity is specific and limited or more general and extended.

Any processor that goes beyond the controller’s instructions and acquires its own role in determining the processing of personal data or the essential means of the processing is no longer a processor, but rather a controller or a joint controller. Art. 28 para. 10 GDPR expressly mentions that the processor will be considered a controller under these circumstances.[[15]](#footnote-16)

* 1. Applicability to ICANN, Registrars, Registries, and Other Third Parties
     1. ICANN’s Roles in gTLD Registration Data Processing

Applying the foregoing criteria, ICANN org should be considered a controller with respect to certain processing activities performed on gTLD registration data, where ICANN org exercises the relevant control. Such processing activities include cases of factual influence, in which ICANN org has the right to audit registration data or to request their transfer for the purpose of transition to another Registrar or Registry pursuant to its agreements with Registrars and Registries respectively.

On the other hand, as explained in further detail below, one possible interpretation is that ICANN org assumes no overall controller responsibility for the processing of gTLD registration data based upon implicit competence (as “naturally attached” to its role). This would be a misinterpretation of ICANN org’s role and the “bottom-up, consensus-driven, multi-stakeholder model” ICANN org is following in its work. Nor does ICANN org have explicit legal competence for the processing of gTLD registration data. So, ICANN org may not be regarded a controller either with respect to the gTLD domain registration − which is administered by Registry Operators and Registrars − or processing activities by registrars related to their contractual obligations with Registrants, or where required by law (*e.g.*, tax law), etc.

* + 1. Registrars are Not Processors

Registrars are not simply agents of ICANN org fulfilling tasks mandated by ICANN org. The agreements concluded by ICANN org with Registrars are subject to a community-based decision process in which representatives of Registrars are fully involved. Registrars have their own purposes in dealing with the gTLD registration data, in particular the fulfillment of the agreements with Registrants, complying with legal requirements (*e.g.*, tax law requirements), etc. Consequently, Registrars based within the EEA are not qualified as processors, but rather as controllers with regard to these processing activities.

Registrars that administer the gTLD registration process, as further stipulated in their agreements with ICANN org, are to be regarded as controllers with regard to these processing activities as well. This assessment is shared by the Art. 29 Working Party who has considered Registrars based within the EEA to be controllers with respect to WHOIS data processing.[[16]](#footnote-17) This assessment is, furthermore, supported by the fact that the reasonable expectations of the data subjects (*i.e.*, the Registrants or their representatives) point to the Registrars as controllers, given that the contractual relationship is between Registrant and Registrar, and not between Registrant and ICANN org.

* + 1. Registries are Not Processors

The Registries within the EEA are controllers for similar reasons as stated above for Registrars.

* + 1. Escrow Providers and Dispute Resolution Providers

In addition to the Registries and Registrars, other parties are involved in the processing of gTLD registration data as controllers or processors. For example, dispute resolution providers are responsible for resolving a wide array of disputes pertaining to domain names. In connection with their roles as *de facto* arbitrators, the Uniform Dispute Resolution Policy (“UDRP”) providers operate as controllers, i.e., they have a degree of control regarding the purposes and means of the personal data they process.

The responsibilities of escrow providers as data controllers or processors requires additional discussion. Some data escrow providers have taken the position that they operate as controllers. On the other hand, other data escrow providers view their role as a data processor of ICANN org and the Registrars or Registries as the escrow provider does not determine the purposes of the processing.

* + 1. Implications if the Contracted Parties Were to be Considered Processors of ICANN org

If the Registries and Registrars were to act just as processors, they would only be able to follow ICANN org’s instructions with regard to the data. Since legal responsibility for lawfulness of the processing falls on the controller and not on the processor, ICANN org and the contracted parties would be required to put a data processing agreement in place, including instructions to a contracted party as processor detailing what it can and cannot do with the data, with the data processing agreement further requiring the processor to only act upon ICANN org’s instructions. In this scenario, ICANN org only would exercise control over both, the purposes for which the data are processed and the means used for this. At the same time, this would result in ICANN org having to put into place costly audit and monitoring systems in order to fulfill its controller responsibilities.

1. Controllership Status is Factually Dependent
   1. Requirements of Joint Control: Determine Purposes and Means Jointly

The GDPR contemplates that parties can either be joint or independent controllers.[[17]](#footnote-18) Whether the parties are regarded as joint or independent controllers is a question that must be legally determined based upon the facts of the processing at issue and cannot be regulated by agreement among the parties.[[18]](#footnote-19)

Furthermore, in assessing joint controllership, “a substantive and functional approach” must be taken “focusing on whether the *purposes* ***and*** *means* are determined by more than one party”.[[19]](#footnote-20) This requires first verifying whether a party has control over the processing and then whether there is joint control with other parties. As the GDPR puts it, “joint controllership” occurs where two or more controllers jointly determine the *purposes* ***and*** *means* of processing.[[20]](#footnote-21)

* 1. Examples of Joint and Independent Controllership

In Opinion 1/2010, the Art. 29 WP provided examples of independent and joint controllership.[[21]](#footnote-22) To illustrate independent controllership, the Art. 29 WP referred to the case of a travel agency sending personal data of its customers to the airlines and a chain of hotels, in order to 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 are three different data controllers, each subject to the data protection obligations relating to its own processing of personal data.

This example of independent controllership contrasts to cases where the travel agency, the hotel chain and the airline decide to set up an internet-based common platform in order to improve their cooperation with regard to travel reservation management. The parties all agree on important elements of the means to be used, such as which data will be stored, how reservations will be allocated and confirmed, and who can have access to the information stored. Furthermore, they decide to share the data of their customers in order to carry out integrated marketing actions. In this case, the travel agency, the airline and the hotel chain, have joint control on how personal data of their respective customers are processed and therefore, will be joint controllers regarding processing operations relating to the internet-based booking platform. However, each of them would still retain sole control with regard to other processing activities, e.g., those relating to the management of their human resources.

The distinction here is that in the latter example, the travel agency, hotel chain and the airline jointly decide on both the purpose and the means of the processing.

In addition, the Advocate General’s recent 19 December 2018 opinion in a case concerning Facebook Ireland and Fashion ID[[22]](#footnote-23) provides a further illustration of joint controllership. In his non-binding opinion[[23]](#footnote-24), the Advocate General proposed that Facebook and Fashion ID, a website operator, should be considered joint controllers, because Fashion ID had embedded a plugin (such as the Facebook Like button) on its website, in turn causing the collection and transmission of users’ personal data to Facebook.

The Advocate General emphasized that a controller’s joint responsibility should be limited to those operations for which it effectively co-determines the means and purposes of the processing of the personal data. In that case, the Advocate General concluded that Fashion ID, the administrator of a Facebook fan page, acted as a controller because Fashion ID contributed to determining the purposes and means of processing the personal data of visitors to the fan page jointly with Facebook Ireland. According to the Attorney General, the commercial and advertising purposes were common to both parties at the time they collect and transmit personal data. Moreover, with respect to the means, by creating the fan page at issue, the administrator gave Facebook Ireland “the opportunity to place cookies on the computer or other device of a person visiting its fan page”, and thus process personal data. The processing at issue enabled Facebook Ireland “to improve its system of advertising” while it provided the administrator with the means to manage better, via anonymized statistics, the promotion of its own activity.

The Advocate General’s opinion is narrowly tailored placing responsibility on the parties only for the operations for which they share or co-determine the purposes and means of processing, and not finding the parties jointly liable for the previous and later stages of the chain of processing where they were not in a position to determine the purposes and means.[[24]](#footnote-25)

* 1. gTLD Registration Processing is Not Just One Set of Operations

Applying the concepts of independent and joint controllership to gTLD registration processing, it is critical to determine whether there is one set of “domain registration” operations or whether the gTLD registration operations should be broken down in different processing activities, which each must be carefully analyzed in order to determine whether it is an independent or joint controller activity. The Initial Report advocates for the former, reasoning that “processing should not be artificially divided into smaller steps, but can be uniformly considered as a set of operations.”[[25]](#footnote-26)

Contrary to the position in the Initial Report, the processing of gTLD registration data consists of various and distinct processing activities, which occur under a common framework of agreements and policies. Such processing activities range from registering a domain name, to safeguarding registration data with EBERO providers, managing domain name disputes, conducting audits and responding to complaints, terminating domain name registrations, and more. While all of these processing activities are done with the overall objective of providing a secure, stable and resilient domain name system, it does not mean, by extension, that the flow of gTLD registration data is a single indistinguishable operating process.

Indeed, not all of the contracted parties and third-party service providers are involved in every gTLD processing activity. For example, Registries and Registrars may transmit domain registration amongst themselves and other third parties such as data escrow agents without ICANN org’s day-to-day involvement. Likewise, some gTLD registration processes may never occur at all such as EBERO services or initiating the dispute resolution process with Uniform Dispute Resolution Policy (“UDRP”) providers. These examples only underscore that gTLD registration processing operations are not “artificially divided”[[26]](#footnote-27), but reflect separate and distinct purposes for processing gTLD registration data, for which the parties play separate and distinct roles.

Moreover, each party exercises independent discretion on the “means” of processing gTLD registration data. For example, the contracted parties decide what technical and organizational measures they use to safeguard domain registration data collected or retained. Additionally, the processing activities of ICANN org and the contracted parties generally happen using different software, applications and systems, different from the above example of joint controllership between travel agency, hotel chain and airline where the parties maintain a joint platform, or the Advocate General’s assessment in the Fashion ID case. This is a critical distinction as it illustrates that each party is determining its own means of processing.

* 1. “ICANN Purposes” Are Not Necessarily Joint Purposes

Rather than analyzing the distinct processing activities that take place in the context of gTLD registration data, the Initial Report refers to what it considers to be “ICANN Purposes” in order to “describe purposes for processing personal data that should be governed by ICANN org via a Consensus Policy.”[[27]](#footnote-28) In effect, the Initial Report assumes that just because a data processing purpose is articulated through contractual terms or adopted through the multi-stakeholder process (in which ICANN org supports and the contracted parties participate), it follows that such purposes are in turn “joint purposes” thereby creating a joint controllership. This analysis yields challenging and undesirable results for several reasons, which should be considered by the EPDP Team.

First, the analysis is inconsistent with the GDPR. A joint purpose between controllers is not determined by an accepted policy, but rather, as explained in Section E below, by a factual analysis on how the controllers jointly determine the specific purpose for processing personal data.

Second and relatedly, it is not determinative that a processing purpose originate from ICANN org, a contracted party, other stakeholders, or applicable laws. Merely because ICANN org may articulate a purpose for a contracted party to process data does not make ICANN org a joint controller with the contracted parties. If that was the case, every technical standard setting body that defines processing protocols for certain personal data would be deemed a controller merely because a third party must adhere to such protocol to be certified compliant with such standards.

Third, the Initial Report has identified cases of gTLD registration data processing as “ICANN Purposes” where the contracted parties pursue different purposes. This is particularly evident with respect to the purposes pursued by ICANN org when conducting audits and inspections, as well as transitioning data from one Registrar/Registry to another, which cannot be shared with Registrars and Registries. By logical extension, these processing activities cannot result in a joint controllership.[[28]](#footnote-29)

Lastly, as noted in Section III.A above, the GDPR has made it clear that joint purpose determinations in and of themselves are not sufficient. The parties also must jointly determine the “means” for such processing. This step requires both ICANN org and the contracted parties to jointly define, implement, and supervise the technical and organizational questions concerning “how” such data will be processed not only at the abstract level of an agreement or policy, but with respect to the concrete processing. Without this analysis, the essential element of control is missing, as discussed below.

* 1. gTLD Registration Data Processing as Controller Activity of Registrars and Registries

As noted above, the concept of controller is a functional concept, intended to allocate responsibilities where there is factual influence[[29]](#footnote-30), i.e., an ability to assume control over the data processing. In Opinion 1/2010 (WP169), the Art. 29 WP sets out a typology of control. The types of control identified are:

* **Explicit legal competence**. When the law imposes an obligation on either public or private entities to retain or provide certain personal data. For example, entities entrusted with certain public tasks (*e.g.*, social security administration) would be considered controllers of the personal data that they collect to fulfill their tasks.[[30]](#footnote-31)
* **Implicit competence**. When the capacity to determine stems from established legal practice. For example, an employer in relation to personal data of its employees or an association in relation to personal data of its members. In other words, when an entity has “implicit competence,” the capacity to determine processing activities is “naturally attached to the functional role of a (private) organization, ultimately entailing responsibilities also from a data protection point of view.”
* **Factual influence**. When based upon an assessment of the factual circumstances, an entity has chosen to process personal data for its own purposes. This may involve an assessment of the contractual relationships of the involved parties. In case of doubt, other elements may be useful to identify the controller, including, for example, the degree of actual control exercised by a party, and the reasonable expectations of Registrants and other individuals based on their relationship and interaction with the entity.

Applying these concepts to gTLD registration data processing activities, ICANN org has neither *explicit* legal nor *implicit* competence to decide about the means of gTLD registration data processing. It furthermore lacks any *factual* influence over the gTLD registration data processing which is administered by Registries and Registrars on systems and applications not under ICANN org’s control. Registries and Registrars determine the actual means of the processing and therefore, are independent controllers with regard to the activities they carry out in accordance with their respective agreements with ICANN org. A Registrar, in particular, is the controller of the registration data it has collected and published in gTLD registration data.

That ICANN org and the contacted parties may come to a common understanding, for example, regarding minimum data elements collected for Registration Data Directory Service (RDDS) or about data retention periods, as agreed upon in the relevant specifications of ICANN agreements, does not change this assessment. This common understanding exists at a consensus level only and is lacking the element of control on the part of ICANN org required to assume control over the data processing in the first place.

* 1. Parties Could Be Independent Controllers

The processing of gTLD registration data consists of various processing activities which occur under a common framework of agreements and policies. Under this framework, where the parties have separate and distinct *purposes* of processing (e.g., selling domain names versus managing top-level domain names), and each party also exercises independent discretion on the *means* of such processing with respect gTLD registration data, the parties are not joint controllers under the GDPR. As such, ICANN org and the contracted parties should consider themselves operating as independent controllers.

1. Implementation Considerations for Independent Controllership

The Initial Report recommends that ICANN org negotiates and enters into a joint controller agreement with the contracted parties. Based on the community comments submitted on the Initial Report, some parts of the ICANN community have recognized the challenges associated with advancing with the EPDP Team’s approach of joint controllership. Most contributors expressing support for the recommendation concerning joint controllership justify their choice by the crucial need to have some clarity surrounding ICANN org and the contracted parties’ roles with respect to each other. For example, some of these commenters note that a joint controller relationship might allow ICANN org to enforce data disclosure requests made under reasonable access requirements and future accredited access requirements. However, at the same time, some of these community comments insist that allocating responsibility among the parties is key, and that it should not be done equally even in the case of a joint controllership agreement. Community commentators expressing support for joint controllership also argue that the joint controller approach should be pursued as it is the best solution absent a sound alternative proposal.

Community comments not supporting the recommendation concerning joint controllership emphasize the fact that proposing a specific legal vehicle (i.e., a joint controller agreement) without adequate consideration of how this would impact ICANN org and the different types of Registries and Registrars that are ICANN org’s contracted parties has the potential to derail the work of the group. These comments recognize that this needs to be a thorough decision that takes into account all elements of the factual and legal analysis.

In addition, brief reference should also be made to the September 2017 memorandum that Wilson Sonsini prepared in response to questions from a prior policy development process to create a new comprehensive WHOIS consensus policy (https://gnso.icann.org/sites/default/files/file/field-file-attach/wsgr-icann-memorandum-25sep17-en.pdf). The memorandum concludes that the parties are joint controllers without proceeding to an in-depth analysis: “It is impossible to set out here how the data controller would be determined for each WHOIS field, since that would involve an evaluation of the complexities of how data are collected and used for each field, and would exceed the scope of this memorandum. Generally speaking, we believe that the best view would be to see each of these entities as a co-controller, i.e., each of them would be regarded as data controller.”

This document attempts to evaluate the factual and legal complexities of the parties’ responsibilities with respect to the processing the various gTLD data processing activities. As discussed in this document, advancing forward with a joint controllership agreement seems not only to run contrary to the parties’ roles with respect to gTLD data processing, but also, as explained below, has significant consequences. Independent controllership is an alternative workable solution.

* 1. Consequences of Joint Controllership

As ICANN org and the contracted parties are aware, joint controllership has far-reaching consequences.[[31]](#footnote-32) Specifically, the GDPR requires joint controllers to enter into a comprehensive arrangement, which can – not must – be of contractual nature, to allocate their responsibilities for compliance with the GDPR in a transparent manner, in particular with regard to exercising of data subject rights and information obligations towards data subjects. The requirement of a joint controller arrangement entails the following risks and disadvantages compared to independent controllership:

* **Implementing a complex joint controllership agreement structure**. The GDPR calls for an arrangement;[[32]](#footnote-33) not necessarily for a contract. While the arrangement can be a single one between ICANN org, the Registries and Registrars, it must define each party’s respective role and responsibilities for compliance with the GDPR. It would also be essential to clearly define and limit the scope of the mandatory joint controller arrangement, *i.e.*, the processing activities for which joint controllership is taking place.[[33]](#footnote-34) Such joint controllership arrangement is not comparable to a simple, more or less standardized data processing agreement pursuant to Art. 28 GDPR in terms of its nature and character. Considering the specifics of the domain name registration system, a joint controllership arrangement for ICANN org and the contracted parties will be complex. It may also, due to its complexity, carry the risk of not being transparent to data subjects, who will hardly understand the various roles and responsibilities of the parties. As such, joint controllership possesses the risk that it fails to comply with the GDPR’s transparency principle.
* **Accepting mandatory joint and several liability**. A joint controllership agreement means that the parties are jointly and severally liable to one another. Any indemnification provisions in a joint controller agreement also would need to attach to defined data processing activities. This further underscores the need for a more practical and commercially viable agreement between the parties that limits the exposure a joint controllership agreement presents.
* **Implementing micro-management of processing and costly oversight, administration and reporting to ensure compliance with the joint controller agreement**. A joint controllership requires ever more careful oversight of each parties’ processing of gTLD data and exposes each parties’ systems and processes to higher scrutiny. This type of micro-management would increase costs and decrease efficiency.
* **Cumbersome audits**. Given the risk profile of joint and several liability, a joint controllership arrangement would likely require the parties to agree to audits and inspections of each other’s processing of gTLD data to ensure compliance with the arrangement, which would be another cost-driver. As independent controllers, however, the parties are more likely to accept that there is no obligation on the part of the controllers to audit and exercise control over the other controllers processing activities, apart from compliance with the common data protection framework and existing agreements.
* **Accepting uncertainty with regard to accountability obligations of the numerous parties involved.** Given the complexity of the processing of gTLD registration data, challenging issues would have to be addressed and hard choices made regarding compliance with the GDPR and the processing of gTLD data. For example, which entities would handle responding to data subjects’ rights or issuing notices to Registrants? As previously mentioned, detailed protocols would have to be developed to ensure that the relevant party timely responds to data subject access requests, which would have to be regularly and routinely monitored for compliance. Other questions arise including with respect to how would parties handle their respective relationships with other third parties.
  1. Advantages of Independent Controllership

Independent controllership as between ICANN org and the contracted parties not only reflects the factual reality of the parties’ relationships, but also offers the greatest flexibility in terms of achieving compliance for several reasons.

* No Required Data Protection Framework. The GDPR does not require any form of arrangement or agreement between independent controllers. Provisions for the relationship between independent controllers as set out in Appendix C of the Temporary Specification are not legally required, but can be beneficial with regard to the weighing of interests required for legitimate interest processing in accordance with Art. 6 para. 1 (f) GDPR as a factor protecting the rights and freedoms of the individuals. Therefore, if the parties decide that they want to implement a data protection framework in order to govern their obligations as independent controllers, they could use a similar framework as in the Temporary Specification using existing defined processes to implement it, instead of having to develop a new framework for joint controllers as envisioned by the EPDP in the Initial Report.
* Flexible Data Protection Framework. As mentioned in the foregoing point, while not strictly required by the GDPR, ICANN org, Registries and Registrars – as independent controllers – may agree on a data protection framework (whether in form of an additional agreement or specification and policy becoming part of the agreements with the contracted parties) applicable to their gTLD data processing. Unlike a joint controller agreement which may be both confusing and lengthy as a result of the parties parsing out their specific responsibilities with respect to gTLD data processing, an independent controller data protection framework provides each controller with greater flexibility to focus on their obligations as controllers with respect to gTLD data in a clearer, streamlined fashion.
* Flexibility in Implementation. When ICANN org and the contracted parties operate as independent controllers, each party has the freedom to address their own respective obligations to comply with the GDPR through any acceptable means, provided such processing is in compliance with the GDPR. This flexibility reflects how ICANN org and the contracted parties regularly operate in practice. While each party may be subject to contractual agreements on gTLD data, Registries and Registrars independently determine how to manage gTLD data and furthermore comply with the GDPR.
* **Additional Benefits**. An independent controller relationship, furthermore, avoids complicated and burdensome discussions regarding typical key features of joint controllership arrangements, as set out in the foregoing section.
  1. Flexibility in Defining Independent Controllership

The GDPR does not contain express requirements how to define and structure the relationship between independent controllers involved in processing under a common framework of agreements and policies. The GDPR offers various possibilities to design those relationships, depending on the circumstances. Such options would include the following:

* + 1. General Rule: The GDPR Applies to Each Controller Independently

For the sake of clarity and increased transparency, any data protection framework (whether in form of an additional agreement or specification and policy becoming part of the agreements with the contracted parties) should make clear that the provisions of the GDPR apply independently to each respective controller involved in the gTLD processing activities who is a signatory or participant to the framework. As such, the framework should further provide that the parties are not joint controllers as defined under the GDPR and thus, not jointly and severally liable for any non-compliance by other signatories.

* + 1. Data Sharing Activities Triggering Information Obligations in Case of Data Subject Requests

Certain data sharing activities among independent controllers trigger obligations, for example, in cases where data subjects exercise their data privacy rights (erasure or rectification). The GDPR requires the controller receiving the request to only notify “recipients to whom the personal data have been disclosed,” i.e., other controllers who have received the data subject’s personal data.[[34]](#footnote-35) It is then the obligation of the other controllers to determine whether they have an obligation to act upon the request of the data subject. For example, if a Registrar receives a request for deletion of personal data from a Registrant, it would delete such data (assuming the other requirements of the deletion request are met) and subsequently inform ICANN org or other Registries and Registrars of this request, thereby facilitating the response by other parties to facilitate an efficient and effective response to the Registrant’s request.

Where data is shared amongst independent controllers, the data protection framework could address and detail how independent controllers will timely respond to data subject requests when they occur and in addition inform each other.

* + 1. Cross-Border Transfer Safeguards

Transfers of EEA personal data outside of the EEA are permitted under the GDPR only under certain circumstances. This includes transfers to countries whose legal regime is deemed by the European Commission to provide for an “adequate” level of personal data protection. In the absence of an adequacy decision, transfers are permitted only if certain safeguards are in place or if a derogation such as consent into the transfer by the data subject applies. For example, independent controllers as group of enterprises engaged in a joint economic activity might agree upon Binding Corporate Rules to safeguard intra company data transfers among them. Likewise, the parties may contemplate the use of EU Controller-to-Controller Standard Contractual Clauses (“SCCs”) to effectuate cross-border data transfers.

However, to the extent the GDPR is directly applicable to the processing activities of ICANN org and the contracted parties in relation to gTLD data processing, developing BCRs or a framework of SCCs to be entered among the parties will not be required.

* + 1. Codes of Conduct

Article 40 para. (2) of the GDPR contemplates that an “organization” representing a group of controllers may draw up codes of conduct “for the purpose of specifying the application of [the GDPR],” that would cover key data protection principles including transparency, accountability, protection measures, the “legitimate interests pursued by controllers,” information to the public and data subjects, and international data transfers, among others. Such codes may even cover more technical and security measures to mitigate the risk of personal data breaches such encryption and pseudonymization. Article 40 para (3) of the GDPR further provides that organizations may extend this code of conduct to other controllers not subject to the GDPR by means of enforceable contracts or other legally binding commitments.

Taking this into account, independent controllers involved in the processing of gTLD data may consider adhering to a code of conduct applicable to their specific processing industry or sector. Another benefit is that any cross-border data transfers to controllers outside of the EEA adhering to an approved code of conduct would be possible without applying transfer safeguards under Art. 46 GDPR.

The UK Information Commissioner’s Office has provided “trade associations or bodies representing a sector can create codes of conduct to help their sector comply with the GDPR in an efficient and cost effective way.”[[35]](#footnote-36) Indeed, prior to the GDPR, some organizations took steps to define common standards for data processing within a category of controllers, while remaining independent. These include:

* Federation of European Direct and Interactive Marketing (“FEDMA”) (EU Direct Marketing)[[36]](#footnote-37)
* German Insurance Industry[[37]](#footnote-38)
* GeoBusiness CoC Self-regulation[[38]](#footnote-39)
* Dutch Financial Industry[[39]](#footnote-40).

ICANN org’s role with respect to the Registries and Registrars as a consensus builder and conductor of the multi-stakeholder process shows some similarities with those organizations listed above.

Taking this into account, a data protection framework built upon a code of conduct will allow ICANN org and the contracted parties far more flexibility to build a data protection regime that complies with the GDPR while also reflecting the parties' independent controller relationship situation. This is a possible approach that ICANN org and the community could potentially explore in the coming years.

* + 1. Impact of Data Protection Framework on Legitimate Interest Processing

If a party’s processing of personal data is based upon legitimate interest as set forth in Article 6 para. 1 (f) of the GDPR (as applicable for certain processing activities in relation to gTLD data processing), a data protection framework (whether in form of an additional agreement or specification and policy becoming part of the agreements with the contracted parties)between the controllers governing their compliance with GDPR obligations would be positively considered in the weighing of interests required for legitimate interest processing as a factor protecting the rights and freedoms of the individuals.

* 1. Consideration of Framework Elements Applicable to Independent Controllership Between ICANN org and the Contracted Parties

The GDPR provides for flexibility in determining how to best address compliance with the GDPR by ICANN org and the contracted parties in the gTLD registration ecosystem. The following are available approaches:

* **Adoption of a uniform data protection specification applicable to ensure compliance with GDPR and existing gTLD registration data consensus policy**. Such specification would become part of each agreement with a contracted party. While the GDPR does not require the adoption of such specification, as it contains no requirement for independent controllers to enter into any form of arrangement or agreement, it seems it would be prudent to continue with the approach taken already in Appendix C of the Temporary Specification and set out relevant independent controller obligations. Appendix C could be further refined to serve as independent controller specification for ICANN org and the contracted parties.
* **Adoption of a code of conduct.** The refined Appendix C of the Temporary Specification containing relevant independent controller obligations could be in the future the basis for a code of conduct pursuant to Art. 40 GDPR. Processing on the basis of a code of conduct would provide greater legal certainty for ICANN org and the contracted parties, as it would require authority approval and oversight by accredited bodies.
* **Limited adjustments in existing agreements**. The parties, as independent controllers could decide to take a very limited approach and only adjust certain data protection related provisions in their existing agreement concerning, for example, notice and consent requirements.[[40]](#footnote-41) However, this might not be the best approach, as it would fail to address other relevant independent controller obligations and a more detailed allocation of responsibilities among the parties in this regard.
* **No arrangement/agreement on independent controller obligations**. As a more streamlined approach is preferred, not agreeing on any independent controller obligations and relying only on community, data subject and data protection engagement, seems the least viable approach.

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

ICANN org would like to thank the EPDP Team for the opportunity to provide additional input on the issue of the roles and responsibilities of ICANN org, registrars and registries with respect to gTLD registration data. 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* ICANN/GNSO, Initial Report of the Temporary Specification for gTLD Registration Data Expedited Policy Development Process, 21 November 2018, *available at* <https://www.icann.org/public-comments/epdp-gtld-registration-data-specs-initial-2018-11-21-en>. [↑](#footnote-ref-2)
2. *Id*. at p. 59. [↑](#footnote-ref-3)
3. *Id.* [↑](#footnote-ref-4)
4. *Id*. [↑](#footnote-ref-5)
5. While Appendix C does not expressly state that the contracted parties are independent controllers, Appendix C is designed to address each party's obligations under the GDPR as independent controllers. It is not intended – nor does it expressly provide – that the parties are engaged in a joint controllership arrangement. [↑](#footnote-ref-6)
6. *See* Art. 3 para. 1 GDPR. [↑](#footnote-ref-7)
7. *See* Art. 3 para. 2 lit. a GDPR. [↑](#footnote-ref-8)
8. *See* ICO: Data controllers and data processors: what the difference is and what the governance implications are (6 May 2014), *available at* <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf>. [↑](#footnote-ref-9)
9. [↑](#footnote-ref-10)
10. *See id.*; *see also* p. 14 WP 169. [↑](#footnote-ref-11)
11. *See* p. 14 WP 169. [↑](#footnote-ref-12)
12. *Id.* at 15. [↑](#footnote-ref-13)
13. *See* Art. 4 (8) GDPR. [↑](#footnote-ref-14)
14. See p. 25 WP 169. [↑](#footnote-ref-15)
15. *See* Art 28(10) (providing that “[w]ithout prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.”). [↑](#footnote-ref-16)
16. *See* Letter of Art. 29 WP to ICANN of January 8, 2014, *available at* <https://www.icann.org/en/system/files/correspondence/kohnstamm-to-jeffrey-08jan14-en.pdf>; *see also* Art. 29 WP Letter to ICANN on the subject of “Comments on the GNSO WHOIS Task Force Preliminary Task Force Report on WHOIS Services of 22 November 2006; and on the Draft ICANN Procedure for Handling WHOIS Conflicts with Privacy Law of 3 December 2006”, dated 12 March 2007, p. 3 *available at* <https://www.icann.org/en/system/files/files/schaar-to-cerf-12mar07-en.pdf> (providing that “A domain name registrar/registry must be considered as a “data controller” in the meaning of the EU Data Protection Directive (article 2-d)”) [↑](#footnote-ref-17)
17. *See* the definition of “controller” in Art. 4 no. 7 GDPR (body who “alone or jointly with others” determines the purposes and means of processing. [↑](#footnote-ref-18)
18. The Opinion 1/2010 on the concepts of “controller“ and “processor“ by the Art. 29 Working Party (WP) (WP169) formulates in this regard that “contractual arrangements can be useful in assessing joint control, but should always be checked against the factual circumstances of the relationship between the parties. ” [↑](#footnote-ref-19)
19. Opinion 1/2010 (WP169), p. 18 (emphasis added). [↑](#footnote-ref-20)
20. *See* Art. 26 para (1) GDPR (emphasis added). [↑](#footnote-ref-21)
21. Opinion 1/2010 (WP169), p. 17 et seqq. [↑](#footnote-ref-22)
22. Case C-40/17 Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV. Although issued in December 2018, the Advocate General’s opinion is based on the EU Data Protection Directive, the GDPR’s predecessor, which, however, already applied a similar concept of joint controllership than contained in the GDPR. <http://curia.europa.eu/juris/document/document.jsf?docid=209357&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=5279874> [↑](#footnote-ref-23)
23. The final decision in the matter will be made by the European Court of Justice which is not bound to follow the Advocate General’s opinion. [↑](#footnote-ref-24)
24. Case C-40/17 Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV., recital 100 et seq. [↑](#footnote-ref-25)
25. *See* supra n. 1 at p. 59. [↑](#footnote-ref-26)
26. *Id.* [↑](#footnote-ref-27)
27. *Id*. at p. 30. [↑](#footnote-ref-28)
28. *See* Initial Report, pp. 57-59. [↑](#footnote-ref-29)
29. Opinion 1/2010 (WP169), p. 9. [↑](#footnote-ref-30)
30. *See* p. 1 WP 169*.* [↑](#footnote-ref-31)
31. *See* for a discussion of the challenges of joint controllership the “ICANN org Comments on 7 November 2018 Memo From Thomas Rickert regarding Processors, Controllers, Co-Controllers and Joint Controllers”, *available at* https://gnso.icann.org/sites/default/files/file/field-file-attach/transcript-epdp-gtld-rd-specs-small-roles-responsibilities-team-12nov18-en.pdf . [↑](#footnote-ref-32)
32. *See* Art. 26 (1) GDPR. [↑](#footnote-ref-33)
33. ICANN org notes that the Initial Report in Annex D takes initial steps to define parties’ responsibilities based on “ICANN purposes,” but seemingly without first identifying which parties are involved in the processing activities and further allocating responsibility to parties not involved in the processing activity at all. [↑](#footnote-ref-34)
34. *See* Art. 19 GDPR. [↑](#footnote-ref-35)
35. *See* UK Information Commission Office, Codes of Conduct, available at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/> (last visited 16 December 2018). [↑](#footnote-ref-36)
36. *See* <https://www.fedma.org/work-areas/self-regulation/>. [↑](#footnote-ref-37)
37. *See* <https://inte.axa.de/site/axade-inte/get/documents/axade/AXA.de_Dokumente_und_Bilder/Footer/Code-of-Conduct.pdf>. [↑](#footnote-ref-38)
38. *See* <https://gdpr.cloudsecurityalliance.org/news/>. [↑](#footnote-ref-39)
39. <https://www.verzekeraars.nl/media/3447/code-of-conduct-for-the-processing-of-personal-data.pdf>. [↑](#footnote-ref-40)
40. *See* Sec. 3.7.7.4 and 3.7.7.5 2013 Registrar Accreditation Agreement. [↑](#footnote-ref-41)