[Date]

Dear Members of the European Data Protection Board,

I am writing on behalf of a multi-stakeholder policy development team formed by ICANN (the Internet Corporation of Assigned Names and Numbers) to develop GDPR-compliant policies to govern the operation and procedures of the domain name industry. The team is approximately half-way through its deliberations, and has carefully read and considered the GDPR, explanatory treatises, and the writings of the EDPB to date. Thus informed, the team has some specific questions where EDPB commentary might inform its remaining work.

Deleted: GDRP

As indicated in Göran Marby's letter of 17 September 2017, ICANN is a global non-governmental non-profit organization that provides for the technical coordination, as well as the stability and security of the Internet's system of unique identifiers, i.e., domain names, IP addresses, and other technical parameters.

Following that letter and considerable work with the ICANN community, on 25 May 2018, the ICANN Board adopted the Temporary Specification for gTLD Registration Data. That Specification, intended to bring the domain name ecosystem into GDPR compliance with the least impact on current operations and practices, will expire on 25 May 2019. Thus, ICANN formed and chartered this Expedited Policy Development Process (EPDP) that is staffed by the ICANN community.

The ICANN community is a volunteer-based, open collection of global stakeholders, including: businesses, Internet engineers, technical experts, civil society, governments (including law enforcement), end users, and domain name registrars and registries. The community works together through a bottom-up process to give advice, make policy recommendations, conduct reviews and propose implementation solutions for common problems within ICANN's mission and scope.

ICANN and the EPDP team have been closely following developing data privacy and protection regulations, to determine the potential impact to the services and functions for which ICANN and domain name registrars and registries are responsible. This includes GDPR's effect on the publicly available Whois database, a globally distributed repository of information, known as registration data, that provides registered domain name holder contact, and other information. In particular, the EPDP Team has been tasked to determine if the Temporary Specification for gTLD Registration Data, which was adopted by the ICANN Board in May 2017, should be adopted as is or with modifications, while complying with the GDPR and other relevant privacy and data protection laws.

Deleted:

To inform its work, the EPDP Team undertook a careful review of each of the data elements collected in the domain name registration process, the purpose for its processing, and the legal basis for that data processing.

The Team has published an Initial Report for public comment describing preliminary recommendations for operating in a GDPR-compliant manner and also answering questions posed in the EPDP Team's Charter. Data Elements Workbooks, which are tools to capture the data processing analysis described above, can be found in the Initial Report Annex.

In its work, the EPDP Team benefited from the advice the EDPB provided to ICANN in previous communications and, in particular, your letter dated 5 July 2018 (see https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf).

We would appreciate any guidance or feedback you may have on the Initial Report. However, the EPDP work contains both factual and legal analysis. We have some specific questions where the EPDP Team is uncertain of GDPR's effect in specific instances and would appreciate your guidance.

I. Designating a third party as a technical or administrative contact

Background:

In your letter of 5 July, the EDPB stated that:

> "The EDPB considers that registrants should in principle not be required to provide personal data directly identifying individual employees (or third parties) fulfilling the administrative or technical functions on behalf of the registrant. Instead, registrants should be provided with the option of providing contact details for persons other than themselves if they wish to delegate these functions and facilitate direct communication with the persons concerned. It should therefore be made clear, as part of the registration process, that the registrant is free to (1) designate the same person as the registrant (or its representative) as the administrative or technical contact; or (2) provide contact information which does not directly identify the administrative or technical contact person concerned (e.g. admin@company.com). For the avoidance of doubt, the EDPB recommends explicitly clarifying this within future updates of the Temporary Specification."

A related footnote states, "[if contact details for persons other than the RNH are provided] it should be ensured that the individual concerned is informed."

Question:

In the case where the registered name holder designates a third party as a contact and provides that person's contact information:

- In accordance with the footnote, is it adequate that registrar informs the registered name holder of her/his duty to inform the third party of any such action?
- If not, is consent, as defined by GDPR, required where the registered name holder designates a third party as a contact and provides that person's contact information?

II. Processing of data that distinguishes between natural and legal person

Background:

The EPDP Team also considered the EDPB Advice in relation to this topic:

> "The GDPR does not apply to the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person. While the contact details of a legal person are outside the scope of the GDPR, the contact details concerning natural persons are within the scope of the GDPR, as well as any other information relating to an identified or identifiable natural person.[1]
>
> The mere fact that a registrant is a legal person does not necessarily justify unlimited publication of personal data relating to natural persons who work for or represent that organization, such as natural persons who manage administrative or technical issues on behalf of the registrant.
>
> For example, the publication of the personal email address of a technical contact person consisting of can reveal information regarding their current employer as well as their role within the organization. Together with the address of the registrant, it may also reveal information about his or her place of work.
>
> In light of these considerations, the EDPB considers that personal data identifying individual employees (or third parties) acting on behalf of the registrant should not be made publically, available by default in the context of WHOIS. If the registrant provides (or the registrar ensures) generic contact email information (e.g. admin@domain.com), the EDPB does not consider that the publication of such data in the context of WHOIS would be unlawful as such."

Question:

The EPDP Team is considering whether it would be possible or desirable to distinguish between natural and legal persons in the context of domain name registrations.

If registrars enable Registered Name Holders to self-identify at the time of registration as a natural or legal person, will the registrar be liable if the registrant incorrectly self-identifies and personal information is publicly displayed? Apart from self-identification, and educational materials to inform the Registered Name Holder, are there any other ways in which risk of liability could be mitigated by registrars?

Deleted: registrants

Deleted: registrant

[1] Article 4(1) GDPR.

III. Lawful bases for processing data – application of Art. 6(1)b vs. 6(1)f

Background:

The EPDP Team considered Art.6(1)b and 6(1)f of the GDPR:

b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(…)
f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

And the Art 29 WP input in relation to this topic:

> "The WP29 wishes to stress that while a particular processing operation might serve several purposes (and therefore can be justified on more than one legal basis), each individual purpose can only be justified with reference to one legal basis. The WP29 therefore encourages ICANN to specify more clearly the envisaged relationship between the legitimate purposes of the processing and the relevant legal bases."

As well as the guidance from the **UK Information Commissioner's Office:**

> ***"When is processing 'necessary' for a contract?***
> *'Necessary' does not mean that the processing must be essential for the purposes of performing a contract or taking relevant pre-contractual steps. However, it must be a targeted and proportionate way of achieving that purpose. This lawful basis does not apply if there are other reasonable and less intrusive ways to meet your contractual obligations or take the steps requested.*
>
> *The processing must be necessary to deliver your side of the contract with this particular person. If the processing is only necessary to maintain your business model more generally, this lawful basis will not apply and you should consider another lawful basis, such as legitimate interests."*

Questions:

The EPDP Team discussed the application of Art.6(1)b vs. Art.6(1)f to the "Purposes for Processing Registration Data" that are identified in the Initial Report. Our questions in this area can best be asked using an illustrative example.

Domain name registrars have contracts with Registered Name Holders (the data subjects) to grant them the use of a domain name that provides a set of functions in the Domain Name System (DNS). With the purpose to ensure that domain names continue to function in the event of a registrar failure (i.e., in the interest of DNS stability), ICANN requires registrars to deposit (disclose) the Registered Name Holders' data with a data escrow agent approved by ICANN. While the registrar might make service level warranties to the Registered Name Holder, the data escrow requirement is not included in the registrar – registered name holder contract.

In selecting a legal basis for the data transfer (deposit) to an escrow agent, the EPDP team discussed the following issues and seeks EDPB guidance on each:

A. Can Art. 6(1)b provide a lawful basis for this purpose (data escrow) even though ICANN does not have a direct contractual relationship with the Registered Name Holder, but ICANN does place certain general requirements on registrars in relation to what needs to be included in the contract that the registrar has with the Registered Name Holder? (The EPDP team agrees that Art.6(1)f applies in this instance but some believe that Art.6(1)b might present a "preferred" legal basis if it applies.)

B. While there are multiple ways a registrar might ensure ongoing, reliable service to a Registered Name Holder in the event of a registrar failure, the ICANN contract between the registrar and ICANN requires that registered name holder data is stored with an outside escrow agent of ICANN's choosing. The guidance from the UK Commissioner's Office seems to indicate that Art.6(1)b would not apply in this set of circumstances as there are other ways to meet this obligation. However, it can be argued that an industry-wide practice is preferable and perhaps "necessary." While the EPDP team agrees that Art.6(1)f applies, some believe that Art.6(1)b also applies and might present a "preferred" legal basis.

C. In relation to Art. 6(1)(b), questions arose regarding how to apply "necessary for the performance of a contract"; specifically, does this clause solely relate to the registration and activation of a domain name registration, or, alternatively, could related activities such as data escrow also be considered necessary for the performance of a contract as a Registered Name Holder should have a reasonable expectation that in case of business failure the domain name registration keeps functioning?

D. As indicated above, the EPDP team is wrestling with whether to select Art.6(1)b or 6(1)f as the lawful basis in the scenario above and in other purposes for processing registration data. Given the clear Art. WP 29 statement above that each individual purpose can only be justified with reference to one legal basis, the EPDP is concerned

Commented [MK1]: I would suggest removing this as it could be read to mean public disclosure, or at least be clear that it is not publicly disclosed (I am not even sure whether the escrow provider has 'access' as such as I believe it was suggested that data is provided in an encrypted format?).

Deleted: r

Deleted: n

Deleted: h

Commented [MK2]: I don't understand what this means?

with the prospect of choosing a lawful basis that is subsequently disallowed by the appropriate authority.

To the extent you are able, please comment on these issues and other guidance in determining when to apply Art.6(1)b vs. Art. 6(1)f.

Please accept our thanks for your time and attention to these questions. Should you have any clarifying questions or would like to discuss these matters or the EPDP Initial Report, please do not hesitate to reach out to me. My contact information is below.

As the Temporary Specification is only enforceable until 25 May 2019, the EPDP Team aims to finalize this report by the end of January 2019 so ideally any feedback you may have is received prior to that. Again, we sincerely thank you for your time and attention to these questions.

On behalf of the EPDP Team,

Kurt Pritz
Chair