Dear All,

The question of “personal data” and “sensitive personal data” under the GDPR is going to come up soon, if it has not already. These are two distinct protected categories of data under the GDPR – and ones that make the line between individual and organizational domain name registrants blurry.

Traditional “personal data,” as you know, is that which can identify a living individual, such as the fields we talk about often in the WHOIS: address, phone, email.

There is a second category of protected data under the GDPR. This is the category of “sensitive data” and sensitive personal data” and its protections are wide-ranging and include protections for fundamental rights including political and religious freedoms.

 “Sensitive” data under the GDPR, per Article 9, includes information pertaining to:

1. racial or ethnic origin,
2. political opinions,
3. religious or philosophical beliefs, or
4. trade union membership,
5. data concerning a natural person’s sex life or sexual orientation shall be prohibited.

See Article 9 of GDPR, *Processing of special categories of personal data,* [*https://gdpr-info.eu/art-9-gdpr/*](https://gdpr-info.eu/art-9-gdpr/)

Data processing of “sensitive data” can take place only for very limited reasons, and always “providing for appropriate safeguards for the fundamental rights and the interests of the data subject.” GDPR Art. 9(2)(b) Thus, those who register a domain name and/or build and run websites for minority racial, ethnic, political, and LGBTQ groups are specially protected.

As you can imagine, this protection of “sensitive data” makes the processing of “legal entities” more complicated than we normally talk about in ICANN – as mosques, synagogues, and increasingly churches today (all generally “legal entities”), among others, are finding themselves exposed to harassment and worse, and expressly protected in their data processing by the GDPR.

**Sensitive data – reaching organizations engaged in a range of fundamental rights**

Despite being “legal entities,” religious, political and LGBTQ organizations are entitled to higher protection for their data to protect the “fundamental rights and the interests of the data subject.” This ensures that the individuals who register their domain names and run their websites receive special protection under the GDPR.

In so doing the line between “individuals” and “legal persons” becomes blurry – especially when the organization are small -- a few people coming together to share minority political concerns, religious beliefs and/or safe sex material (and as we know, most organizations will pass through this “small stage” of a few individuals before becoming the large, well- established organizations we come to know later). The GDPR recognizes that these organizations, even if technically “legal persons,” are exposed and the individuals who assist them, including as DN registrants, are vulnerable.

I’ve talked extensively with Council of Europe’s Data Protect1ion Unit about these “sensitive data” protections under the GDPR, and they were the ones who pointed out these additional protections under the GDPR to me. I would be happy to provide you with more information, if you would like.

**Edits to the EPDP Draft**

In all events, I would like to urge that the EPDP drafting document include references – many of them – not only to “personal data” but to “sensitive data.” This is consistent and required by the GDPR and this inclusion will serve as an important flag for those serving on the upcoming EPDP. It will let them know to dive more deeply into Article 9 of the GDPR and its sensitive data protections – and explore more closely why the ICANN Board chose not to differentiate between legal persons and individuals in the Temporary Specification.

Such inclusion of “sensitive data” will also make it clear how much needs to go into an evaluation of the “access to registration data based on legitimate interests not outweighed by the fundamental rights of relevant data subjects.” It will not be an easy or clear evaluation – especially with the types of organizations we have identified above!

One example of edits to the EPDP draft is set out below.

Please let me know what I can do to help!

Best, Kathy

----------------

Annex:

Suggested edit to Page 2, *Part 1: Purposes for Processing Registration Data,* please see recommended edits in green:

[Note: Questions under a) are gating questions for ~~Phase 2~~ the EPDP Team’s discussion of access, in that they must be answered before work on an access model can commence. They are gating because establishing purposes will inform decisions about how personal registration and sensitive registration data is processed. Because providing access to non-public personal and sensitive registration data is a processing activity, there must be a legitimate purpose(s) with a corresponding legal basis(es) established.