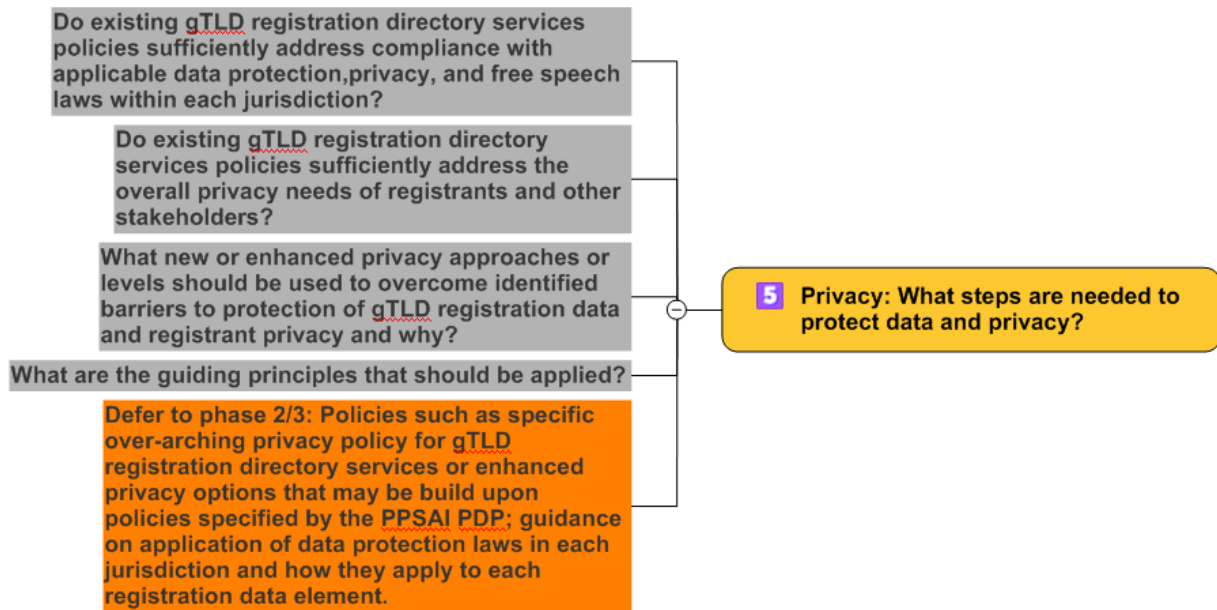


5. Charter Question: Privacy



The following principles are excerpted from *Data Protection & Privacy Principles for the RDS PDP WG*, to inform deliberation on this charter question and related sub-questions. Principle numbers may be used to map back to the [source documents](#) and to the [WG questions](#) asked of senior EU privacy experts and independent legal counsel.

5.1 Do existing gTLD registration directory services policies sufficiently address compliance with applicable data protection, privacy, and free speech laws within each jurisdiction?

3.e. The GDPR applies to all personal data.

3.f. The data of legal persons (their name and form as well as their contact details) are not covered by the GDPR (but as noted above, personal data listed as contact information for a legal person is covered by the GDPR).

9.c. Anonymous public access to registration data may have some potential beneficial use with regard to consumer protection but it cannot by itself override the fundamental right to data protection. (see also principle #8.b.)

12.a. Neither the Article 29 Working Party nor the European Data Protection Board (EDPB) take into account foreign laws when ruling on a case. This reflects the emphasis in the GDPR on the fact that evaluation of data protection rights must be subject solely to EU or Member State law.

13.a. The GDPR applies to data controllers or data processors not established in the EU when their data processing activities are related to "(a) the offering of goods or services, irrespective of whether a

**Data Protection and Privacy Principles, Mapped to Charter Question on Privacy
Handout for 3 October 2017 RDS PDP WG Call**

payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union”.

13.b. The CJEU has granted overriding status to both EU law and the fundamental right to data protection when they conflict with other legal systems.

13.c. Bringing the data processing practices of ICANN and the registrars in line with EU data protection law as much as possible, and giving primacy to EU data protection requirements when they clash with those of other jurisdictions, [would reduce conflicts with local law.]

14.a. Both the national DPAs and the EDPB will have jurisdiction over all types of entities (including registries, registrants, registrars, etc.) that are within the GDPR’s material and territorial scope.

14.b. The GDPR has extraterritorial scope, so national DPAs and the EDPB can take enforcement action with regard to activities performed outside the EU. However, the DPAs and the EDPB may not directly enforce EU data protection law outside the territory of the EU.

16.a. Since the GDPR will come into force in less than a year, it is imperative that ICANN orient its policies and practices around that rather than national laws.

5.2 Do existing gTLD registration directory services policies sufficiently address the overall privacy needs of registrants and other stakeholders?

No principles identified

5.3 What new or enhanced privacy approaches or levels should be used to overcome identified barriers to protection of gTLD registration data and registrant privacy and why?

1.h. Individuals must be provided with adequate information so that they may understand the extent to which their data are being processed.

1.i. If processing is based on the consent of the individual, the individual must be “informed” for their consent to be valid.

11.a. Consent is restrictively defined in the GDPR: Consent needs to be unambiguous, free (freely given), informed and specific. Consent is not a waiver for disproportionate or unlawful processing.

11.b. To satisfy these criteria, consent would have to (1) be implemented in a granular fashion; (2) clearly set out the purposes of data processing; (3) provide the individual with information about how their data will be processed before the data are collected; (4) be expressed in a clear and unambiguous fashion; and (5) be revocable.

**Data Protection and Privacy Principles, Mapped to Charter Question on Privacy
Handout for 3 October 2017 RDS PDP WG Call**

11.d. Consent for further uses of registration data should be separate from any consent for the registration of a domain name (i.e., individuals should be able to consent to register domains without being forced to consent to further use of their data as well).

11.e. Clear information would have to be provided to individuals about the implications of their consent, and would have to be clearly phrased.

11.f. Procedures would have to be put in place to deal with cases when individuals wanted to withdraw or revoke their consent. The withdrawal of consent does not affect the legality of data processing prior to withdrawal. The GDPR does not address the consequences of withdrawal of consent, and withdrawal must be possible at any time.

5.4 What are the guiding principles that should be applied?

1.b. The entity that decides the means and the purposes of processing personal data is the data controller. The role of data controller may be a shared responsibility (see later principles).

1.c. The data controller's role in deciding the means and the purposes of processing personal data is a prerequisite for compliance with other principles, such as data quality, data minimization and transparency.

1.e. Each purpose requires its own legal basis for processing.

2.b. Legal bases (grounds) for data processing can include the individual's consent, necessity to perform a contract, compliance with a legal obligation, and the data controller's legitimate interest, among others. The two that are relevant [to registration data] are the consent of the individual and legitimate interest of the data controller unless this is overridden by the fundamental rights and freedoms of the individual. Consent is a stable legal basis that could be used for the processing of registration data by data controllers. Note that specific requirements exist with regard to how consent is expected to be obtained (See also principles for Question 11 below.)

2.c. The conditions for application of the "legitimate interest" grounds are restrictive and uncertain, and would be unlikely to be found applicable to all the possible uses to which registration data could be put. (see also question #15)

10.a. Even if the processing is founded on a correct legal basis, this does not exempt controllers from respecting the entire set of data protection principles (including fairness and proportionality).

11.c. GDPR's requirements will apply to all data processing that takes place as of its entry into force. This means that, if personal data have been collected before that date, their subsequent processing will still be subject to the GDPR.

17.a. The data controller is the entity that decides the purposes and the means of the processing, and a data processor conducts the processing exclusively on behalf and at the instruction of the data controller. (see also principle #1.b.)

**Data Protection and Privacy Principles, Mapped to Charter Question on Privacy
Handout for 3 October 2017 RDS PDP WG Call**

- 17.b. Where one or more entities decide the purposes, they may be joint controllers.
- 17.c. It is also possible that the same entity is a controller for one purpose, and a processor for another.
- 17.d. ICANN is a data controller to the extent that it autonomously decides and imposes its policy on the other entities involved.
- 17.e. Under Article 4(7) GDPR, in the current model, registries, registrars, or any other parties that determine the purposes and means of how data will be processed in the domain name system could each be a data controller.
- 17.f. All parties that would act as joint controllers should implement an “arrangement” to govern matters such as “their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14” (Article 26(1)).

WG Agreements on Privacy

The following WG agreements to date are excerpted from [KeyConceptsDeliberation-WorkingDraft-26Sept2017.pdf](#)

14. [For MPDS] Existing gTLD RDS policies do NOT sufficiently address compliance with applicable data protection, privacy, and free speech laws about purpose