# Privacy Committee Charter

## Draft Proposal for Review

*Subject to approval by the Board.*

## Background

**Data**: DNS-OARC encourages the collection of various datasets related to the DNS, mainly from its members. The datasets are made available to DNS-OARC members for research and analysis purposes, for example to gain insight into operational practices and deployment challenges. The results of the studies are in general presented to the DNS-OARC community, or DNS community at-large. As such, the datasets are a major asset of DNS-OARC enabling community research and analysis, thus contributing directly to the goals of OARC's core function.

**Data Storage:** These datasets are stored and curated by DNS-OARC on bare-metal systems that it manages in third-party data centres. DNS-OARC controls access to data and aims to enforce restrictions on how data is used. The principal mechanisms used to control access to and use of data is the membership agreement executed between individual members and DNS-OARC.

**Risks:** The extent to which DNS-OARC's data governance practices comply with privacy legislation in Canada and California (where datasets are stored) and Europe (where applicable) is unknown. DNS-OARC's responsibilities with regard to data protection are not well-understood by members or staff. The risks associated with this low level of preparedness for the organisation are not well-understood.

**Single Policy:** Datasets curated by DNS-OARC are effectively managed under a single policy. It is not currently possible for individual datasets to have dataset-specific licenses for storage, access or use. Changing policies around data access or use involves an expensive and time-consuming process of renegotiating legal agreements with individual members.

**Future use of cloud platforms:** All datasets curated by DNS-OARC are stored on and accessed via bare-metal systems operated by DNS-OARC. In recent years, many "big data" applications have migrated away from self-maintained infrastructure to shared, cloud-based infrastructure and there is a significant and growing ecosystem of analysis tools and capabilities that provide advantages by doing so, including applications that have stringent requirements for the handling of sensitive and personal data such as those relating to healthcare. It is not clear whether DNS-OARC's current practices in this regard provide the best balance between flexibility, accessibility, privacy and security.

**Public Services**: There are public services provided by OARC (DNSViz, the website, Mattermost chat) which are not covered by the participation agreement and currently have no privacy policy at all.

A privacy committee has been formed to explore these issues.

Open Question: The participation agreement differentiates between ‘Data’ (e.g. DITL) and ‘Information’ (verbal and/or written information shared with DNS-OARC Participants). Does the definition of this distinction or any management of this ‘Information’ fall within the scope of the committee’s charter?

# Goals

The goals of the Privacy Committee include:

1. Obtain informed and reliable opinions about the degree to which DNS-OARC currently satisfies the requirements of relevant privacy law for data (as defined above).
    a. if there are areas in which DNS-OARC is not currently compliant, identify remedial actions that could be taken to make DNS-OARC compliant with relevant privacy law,
2. Within the constraints of relevant privacy law, consider how to maximise the amount, usability and usage of data (as defined above) collected by OARC in future.
    a. Explore opportunities to allow different policies for storage, access and use of individual datasets, and assess whether such flexibility would be useful and practical.
    b. Explore opportunities for some datasets to be stored and managed in, and accessible to researchers from cloud-based data lakes as an alternative to being stored on DNS-OARC’s own systems.
3. Given the different sources and types of datasets, the definition of metadata can simplify access to data. Metadata can describe the dataset and possibly the relevant policies for accessing and using the data. A task force may be tasked with working on metadata and requirements for a maintained data catalogue.
4. Review the coverage required for any privacy policy related to public services and work with an appropriate professional (e.g. a privacy lawer) to develop and publish such a policy.
5. Propose a process for appointing a Privacy Officer

## Non-Goals

The following topics are explicitly excluded from the Privacy Committee's work in the interests of avoiding scope creep:

1. Drafting, reviewing or proposing specific legal text to incorporate in the DNS-OARC membership agreement or other legal documents; the committee may, however, recommend that such work be done by qualified legal personnel.

## Members

The Privacy Committee includes:

- Jaromír Talíř <jaromir.talir@nic.cz>
- Benno Overeinder <benno@NLnetLabs.nl>
- George Michaelson <ggm@algebras.org>
- Dave Lawrence <tale@dd.org>
- Sara Dickinson <sara@sinodun.com>
- Joe Abley <jabley@hopcount.ca>
- Shivan Kaul Sahib <shivankaulsahib@gmail.com>

The members of the Privacy Committee represent a broad diversity of rich experience. However, it is expected that there will be some areas pertinent to the work of the Committee where additional expertise is required, for example in the general area of privacy controls or in exploration of facilities available in particular cloud platforms. The Committee will call upon external experts to provide advice where appropriate.

## Milestones

Many of the following, once agreed, will need dates. But it seems more important to agree on what the milestones are before proposing any.

- Produce a short report cataloguing
    - Current data storage (number of organisations, types of data shared, etc.)
    - Known data usage to date (how many accesses, usage of analysis resources, publications)
- Report any suspected deficiencies in DNS-OARC's compliance with privacy law to the DNS-OARC board so that the board can make informed decisions about how to investigate further and determine whether corrective action is appropriate.
- Provide guidance to the members describing how to make use of OARC data, e.g. how to publish derivative datasets or information about them, etc
- Make regular reports to the DNS-OARC membership about progress and any open issues of discussion.
- Conduct surveys of the membership to inform decisions about direction, where appropriate.

- Make recommendations to the DNS-OARC board about any structural changes that should be made in existing membership agreements.
- Make recommendations to the DNS-OARC board about infrastructure strategy with regards to data storage, access and use.