DIRECTORATE GENERAL
HUMAN RIGHTS AND RULE OF LAW

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

INFORMATION SOCIETY DEPARTMENT
DATA PROTECTION UNIT

Privacy and data protection principles guide

for ICANN related data processing

October 2017

The present guide is intended[1] to support the integration of, and the compliance with, internationally recognised privacy and data protection principles.

1. Definitions (see Annex)

As a starting point, it is of the utmost importance that the main concepts and definitions regarding privacy and data protection are commonly understood. Although there can be slight differences in some jurisdictions, **personal data** is any information relating to an identified or identifiable individual. It is to be noted that in most of the jurisdictions, data of legal persons are not considered as personal data, except if they enable the identification of a natural person. In an ICANN context, even thin WHOIS data, IP addresses (including dynamic ones), metadata, etc. are to be considered personal data as the identification of an individual by using such data or by combining them with other publicly, easily accessible data is possible.

As for **data processing**, it should be noted that every action which is carried out on personal data, even if it is part of a complex technical operation, or where it consists of the maintenance of a public registry, is considered to be a processing.

In order to define who is the **data controller** (the one who will be held responsible), in the highly complex network of operation of ICANN, one should focus on the level or localisation in the system of the decision-making power regarding the data processing. When it comes to the specific actions performed to the data (during regular operations) the one making key decisions as to the processing of data (for instance determining the reasons justifying the processing, its purposes and the means used for it, having control over the processing methods, the choice of data to be processed and who is allowed to access it) is qualified as the data controller. Looking at this decision-making power more closely, it can be demonstrated in some cases that not only one but two or several organisations have decisive powers, as joint-controllers. As such, they have common and shared responsibilities towards the data processing.

[1] in accordance with Paragraph 9 of the Declaration of the Committee of Ministers of the Council of Europe on ICANN, human rights and the rule of law (3 June 2015).

2. Purpose statement

Before any data processing is carried out, a clear purpose statement has to be defined in order to respond to the requirement subjecting the processing of personal data to predefined and specific purposes. One needs to ask why is the organisation processing personal data? In an ICANN context this would entail at least two purpose statements related to registrants' data: one related to the ICANN policy for which the data is processed and one for the contracted party who will enter into a contract with the data subject, the registrant. The purpose statement has to be developed by the data controller, in case of joint-controllers, there has to be an arrangement between the two or multiple controllers regarding who is processing data for which purposes and to what extent.

A purpose statement can contain all the legitimate reasons for which an organisation would process personal data. Some precaution is necessary when listing those purposes as a data controller is (and could be held) accountable for all the data processing it performs according this purpose statement. On the other hand, if data are being processed for purposes which are not stated in the purpose statement, in most of the cases it will mean that the processing is out of purpose, and thus unlawful. A purpose statement can be modified or adjusted over time, but as a general principle it should be in line with the organisation's mission, powers, mandate, business plan, etc. It should not be very lengthy but it should always contain in a relatively detailed way all the legitimate purposes the organisation wishes to process the data for, including all possible use and reuse after collection.

In conclusion, one organisation is to define its own purpose statement and should not process personal data which do not fall into these purposes (even if data is known or likely to be useful for other organisations).

3. Processing of personal data

After the purpose statement has been defined, it is advisable to map all the data processing activities the organisation will undertake during its operations, indicating the legal basis for each operation, as well as all possible personal data which will be needed for those operations. When finalising the mapping, a final adjustment of the three elements (data processing – legal basis – personal data) according to the predefined purpose statement needs to be done in order to only keep data which are relevant and proportionate.

For example, if the **purpose** of the data processing is the maintenance of the domain name system, which involves a complex set of operations, it is extremely important that the controller predefines which personal data it will process at which stage of its operations, on which ground and for what reason. Like this, it will be easier to assess why it would need to process for example the physical address of a registrant and for which of its operations it would use this specific data and what is the rationale behind it.

One should note that in every international and national legislation in the field, **exceptions** are foreseen where the rights to privacy and data protection can be limited. These exceptions are usually related to cases where personal data are processed for national security, defence, public safety, law enforcement purposes or when such a limitation is necessary for the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression. It is to be noted nevertheless that it does not mean that personal data can be processed for these purposes without limitation or that those purposes can be "freely" added to the purpose statement, but it rather means that if the law provides for such exceptions in certain specific cases, the data controller can apply different rules to the processing of those data for those purposes.

On data processing: as a general rule all data processing has to comply with the **necessity, proportionality and purpose limitation** principles. This implies the pre-existence of clear and legitimate purposes and that the processing should be necessary and proportionate to these legitimate purposes. The data processing should furthermore be carried out **lawfully, fairly and in a transparent** manner. Further use of data is considered as a new data processing therefore the same measures and conditions are applicable for this type of processing as well. Data controllers shall take appropriate **security** measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data. The controller shall notify those data breaches at least to the competent national body (ex: supervisory authority entrusted with the enforcement of the data protection law) which may seriously interfere with the rights and fundamental freedoms of data subjects.

On the legal basis: it should be noted that consent is only one of the possible legal basis allowing a controller to process personal data. It seems that in an ICANN environment, the data processing based on consent is practically impossible as in case of non-consent the same service would not be provided to the data subject, which means that the consent can never be freely (and unconditionally) given. Therefore it would be worth exploring other legal basis for the processing of personal data more suitable for the ICANN context, in particular the one related to the performance of contractual obligations.

On personal data: personal data processed shall be accurate and up-to-date to ensure the highest data quality possible and shall be stored in a secure way only for as long as necessary for the legitimate purpose pursued. It should furthermore be adequate, relevant and non-excessive in relation to the purposes of the processing. If **special categories of data** ("sensitive data") are processed it should be noted that generally, an extra care and protection when handling such data are required, and often national legislations foresee that appropriate (legal and technical) safeguards are to be put in place in order to guard against the risks that the processing of such data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.

4. Transparency

Transparency is an essential requirement a data controller should comply with in relation to its data processing activities. It implies that a data controller should give sufficient information to data subjects regarding the processing activities it will undertake during its operations. Besides, detailed information has to be made accessible for data subjects on the data processing activities and on the manner in which to exercise their rights.

For ICANN, one manner to comply with this requirement could be the creation of a dedicated web-space where all the information about the data processing ICANN is carrying out can be found in an easily understandable way and where data subjects are given the possibility and explanation on how to address ICANN for exercising their rights.

5. Data subjects' rights

As a general principle, data subjects have to be in control of their personal data, which basically means that the data processing shall be in accordance with the data subject's will. It implies that the data subject has to be adequately informed about what will happen with her/his data and has to be granted specific rights in order to remain in control of the data. Such rights apply throughout the entire lifecycle of the data, no matter the number of data processing actions or data controllers processing the data. Those rights, to be exercised at any time, are the rights of access, right to object, right to erasure, right to correction, and right of redress. In some jurisdictions there can exist other rights: right of blocking, right of portability, right to know the reasoning of the processing, right to de-indexing, right to be forgotten, etc.

When it comes to the ICANN context, it would be required that a comprehensive information chart on the data processing operations is brought to the attention of the data subjects both by ICANN and the contracted parties. Besides, it would be highly recommended to put in place an easily accessible procedure or mechanism enabling the data subjects to exercise their rights in individual cases (access request form and contact information, remedies available, etc.).

6. Storage of data

The storage of data aims at achieving the purpose of the processing. As the data is always collected for a specific purpose it is logical to only keep such data for as long as it serves this purpose. Data which do not serve the purpose anymore shall be permanently deleted.

In the ICANN context, it would be desirable to develop an organisation-wide policy for the storage of data (disposal and retention scheme indicating the maximum period of storage for a particular purpose) which would also contain a review mechanism to check whether stored data still serve the purpose they were collected for. Contracted parties should follow their data storage policies according to the applicable law.

7. Trans-border transfer of data

Data transferred to another country should always be afforded an equivalent level of data protection, which implies that the transfer of personal data may only take place where an appropriate level of protection is secured by the recipient. It can be done by international or national legal instruments, ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments. Exceptions may apply, but are to be interpreted narrowly and in specific individual cases.

ICANN as a global organisation should have its own data transfer policy. The applicable rules and/or regimes for trans-border data transfer will largely depend on the contractual relations ICANN has and will have with its contracted parties. Anyhow, ICANN should approve ad hoc or standardised safeguards which could be used by the organisation itself for trans-border data flows but also by contracted parties, no matter their geographical location.

8. Accountability

Data controllers are responsible for the data processing they carry out, which means that they shall pursue their activity in compliance with the applicable legislation. This compliance has to be demonstrable at all times and in relation to every data processing activity which involves personal data.

To comply with this requirement ICANN should, besides putting into place the mechanisms discussed under points 4 and 7, integrate in its policy making processes considerations which enable the organisation to be able to demonstrate its compliance with the applicable law. This can be achieved in various forms, but for policy making processes which concern large amounts of personal data or where the risk that the policy will affect in a considerable way data subjects' privacy is significant, a "Privacy Impact Assessment" is recommended.

9. Privacy by design and privacy by default

In order to better guarantee an effective level of protection, controllers should assess the likely effect of the processing of personal data on the rights and freedoms of the data subjects before beginning the processing. In addition, they are obliged to design the data processing in such a way as to minimise the risk of interference with those rights and freedoms, ensuring that data protection requirements and the protection of data subjects' rights are integrated as early as possible – i.e. ideally at the stage of architecture and system design – in data processing operations through technical and organisational measures.

ICANN should develop recommendations aimed at enhancing the application of these principles into its policymaking and internal processes.

ANNEX

For the purposes of this Guide:

a. “data processing” means any operation or set of operations which is performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data;

b. “controller” means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has the decision-making power with respect to data processing;

c. “joint-controllers” means, for a single processing operation, the various parties which jointly determine the purpose and the means of the processing to be carried out and are therefore in such a case "co-controllers” considered as being constrained by the obligations imposed by the applicable law;

d. “personal data” means any information relating to an identified or identifiable individual (“data subject”);

e. “recipient” means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;

f. “special categories of data” means genetic data; personal data relating to offences, criminal proceedings and convictions, and related security measures; biometric data uniquely identifying a person; personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union members.