COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 7 September / septembre 2018 T-PD(2018)18 Final

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

PRIVACY AND DATA PROTECTION PRINCIPLES GUIDE

FOR ICANN RELATED DATA PROCESSING

Directorate General of Human Rights and the Rule of Law

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, or the escrowing of such data is considered to be a processing.

In order to define who the **data controller** is in the highly complex network of operations 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 more organisations have decisive powers, as joint-controllers. As such, they have common and shared responsibilities towards the data processing.

2. Purpose specification

According to the purpose specification principle personal data shall only be processed for explicit, specified and legitimate purposes and shall not be processed in a way incompatible with those purposes. It is to be noted that various tools are at the disposal of the data controllers in order to comply with this principle.

In order to contribute to a high degree of accountability, data controllers are encouraged to define, before any data processing is carried out, a clear purpose statement. 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 to 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 and business plan. 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(s) and reuse(s) after collection.

[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).

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 the 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 and/or 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. It is to be stressed that competent authorities such as law enforcement authorities may have access to personal data held in public or private registries under lawful procedures and in accordance with applicable national and international law where this is in the public interest (e.g. maintenance of public order or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties).**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. The further use of data is considered to be a new data processing activity; 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 record data breaches which may seriously interfere with the rights and fundamental freedoms of registrants or other data subjects and notify the competent national body (for instance, the supervisory authority entrusted with the enforcement of the data protection law in that jurisdiction) and possibly to the data subjects themselves where the breach is likely to result in a significant risk for them.

On the legal basis: it should be noted that processing on the basis of free, specific, informed and unambiguous consent is only one possible legal basis allowing a controller to process personal data. It seems that in an ICANN environment, processing data based on consent can be challenging as consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations. Therefore it

would be worth exploring other legal basis for the processing of personal data more suitable for the ICANN context.

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 manner only for as long as is necessary for the legitimate purpose pursued. The data 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 the modernised Convention for the protection of individuals with regard to automatic processing of personal data (modernised Convention 108)[2], requires an extra care and protection under the form of appropriate safeguards when handling such data.

4. Transparency

Transparency is an essential requirement that 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 – if no exceptions or derogations apply – regarding the processing of activities it will undertake during its operations, i.e. before it starts the processing (right of information of the data subjects). 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 contact ICANN in order to exercise their rights. Such a resource should be accessible in multiple languages.

5. Data subjects' rights

As a general principle, data subjects have to be in control of their personal data, which 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 which can be exercised at any time – if no exceptions or derogations apply – according to Article 9 of the modernised Convention 108, are the right of access, the right not to be subject to a decision significantly affecting him or her solely based solely on an automated processing of data without having his or her views taken into consideration, right to object, right to erasure, right to correction, and right of redress. In some jurisdictions there can exist other rights: for instance, the right of blocking, right of portability, right to know the reasoning of the processing, right to de-indexing and the right to be forgotten among others.

In an ICANN context, it would be required that a comprehensive information chart on the data processing operations be brought to the attention of the data subjects both by ICANN and the contracted parties. In addition, it would be highly recommended to put in place an easily accessible procedure or mechanism enabling the data subjects to exercise their rights without excessive delay or expense in individual cases (for example, a multilingual access request form and contact information, remedies available among others).

6. Storage of data

The storage of data aims at achieving the purpose of the processing. As the data is always collected for a

[2] Convention 108 as amended by Protocol CETS 223:
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

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 an 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. Transborder transfer of data

Data should only be transferred to another country if an appropriate level of data protection is guaranteed. The means by which an appropriate level of data protection can be secured can vary; it can be done by the law of the state to which data are transferred including applicable international treaties and agreements , or 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 cases.

ICANN as a global organisation should have its own data transfer policy. The applicable rules and/or regimes for transborder data transfer will largely depend on the contractual relations ICANN has and will have with its contracted parties which are or will be created within the applicable national and international legal framework. ICANN should use 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. It notably implies that data controllers take all appropriate measures to comply with privacy and data protection principles described in this Guide and be able to demonstrate such compliance, for example using the purpose statement with respect to the compliance with the purpose specification principle.

A possible measure to facilitate the demonstration of compliance with privacy and data protection requirements can be the designation of a “data protection officer” entrusted with the necessary means to fulfil his or her mandate.

Furthermore, where internal policies are being developed that may result, after careful examination, in data processing which can represent a risk of interference with individuals’ rights and freedoms (ex: it constitutes a high risk to the violation of a data subject’s rights to privacy and/or data protection), it is recommended so as to prevent or minimise the risk of interference with those rights and fundamental freedoms that an impact assessment be conducted and dedicated privacy policies for different types of data processing be developed.

9. Privacy by design and privacy by default

In order to better guarantee an effective level of protection, data 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 (“joint controller”), has the decision-making power with respect to data processing;

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

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

e. “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 membership, religious or other beliefs, health or sexual life.