Ref. Ares(2018)723756 - 07/02/2018

EUROPEAN COMMISSION

Technical input on proposed WHOIS Models on behalf of the European Union

1. INTRODUCTION

The Commission welcomes the concrete proposals set out by ICANN in its "*Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation – For Discussion*", prepared by ICANN Org and published on 12 January 2018, as well as ICANN's commitment to "*ensure compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible.*"[1]. As indicated in previous interactions, developing concrete options facilitates the assessment, also for the necessary compliance review with EU data protection law (in particular the General Data Protection Regulation (GDPR)). It is important to recall that, where compliance questions arise, it will be for the Member States data protection authorities and ultimately for the courts at national and EU level to clarify the interpretation and application of these rules.

The proposed models are therefore considered as a helpful step forward and the Commission welcomes the efforts currently under way to reach out to and engage in a dialogue with the data protection authorities. At the same time, given the importance of determining the best approach in light of the important interests at stake and the many stakeholders concerned, we consider that it would be better to delay ICANN's final decision on the interim model while keeping the current momentum, so that it is possible to arrive at a good solution for all parties involved. Deferring the decision until after ICANN61 would allow for discussion with all stakeholders involved as well as the data protection authorities, which can only usefully take place now that concrete models have been put forward for consideration.

In the following, the Commission sets out a number of considerations that it urges ICANN to take into account when designing a model for future data processing that ensures full compliance with the EU data protection rules.

[1] Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation. Page 2.

In summary, in light of these considerations and without prejudice to the final decision resulting from the on-going analysis and consultation process, a combination of various elements from the models, all of which contain positive and negative elements, could be the best solution.

2. OBSERVATIONS ON THE DIFFERENT MODELS

The Commission takes note of the efforts of ICANN to develop a layered approach as regards the access to the data in the WHOIS directory, which could help to address a longstanding request of the EU Member States data protection authorities. However, given the level of abstraction of the models, it is difficult to assess the scope and impacts of the proposed approaches. The Commission therefore encourages ICANN to further develop possible options in cooperation with the community in order to balance the various legal requirements, needs and interests.

Not all of the relevant design elements are necessarily linked to any specific model. For instance, different data retention periods have been chosen for the different models, without any particular justification. The same holds true for the conditions for access to non-public data. While we fail to understand why a certain retention period or certain access criteria are linked to a particular model, it is clear that, as retention and access (but also the initial data collection) are all forms of data processing, their scope and limits will be determined by factors such as the legitimate purpose, legal basis and proportionality of processing. Therefore, the Commission will not comment on the models as such but rather on the different elements in the models separately.

Purpose definition

The Commission notes the efforts undertaken by ICANN and its community to define clear purposes for WHOIS based on the objectives set out in the underlying Bylaws and contracts and the legitimate interests pursued. This is an important step and a pre-requisite in advancing in the work towards compliance with the GDPR.

At the same time, we still note some confusion between purposes and the legal basis for processing (such as the performance of a contract or legitimate interest). The data protection rules require the purposes for the processing of personal data to be specified and explicit (Article 5(1)(b) GDPR). Such purposes, which include the pursuit of certain public policy objectives (such as the prevention, detection and investigation of crimes) in the legitimate interest of the controller or third parties, should be clearly and explicitly set out in policy rules and defined with more granularity, explaining how they relate to specific processing activities (e.g. collection, storage, publication, access).

Registrants should be informed in a clear and easily understandable manner about these purposes and the related data processing when making, updating or extending

registrations in line with the principle of transparency as elaborated in Article 13 of the GDPR.

Data collection

On page 4, the commonalities across all models are listed. The Commission notes that the use of the word "may" in the first two bullet points indicates that there is a choice for the registrars, which implies that some may choose not to collect the data. It is important to provide clarity and legal certainty here. In line with the aim to preserve the functioning of the WHOIS to the greatest extent possible, the obligation to collect the data under ICANN rules should cover the maximum permissible, taking into account the necessity for data collection resulting from the respective purpose(s) of processing and the available legal basis (which may include, for instance, the performance of a contract and/or the legitimate interests pursued by the controller or by a third party),.

Data retention

The data retention period for the different categories of personal data should be based on individual business needs and a proper data protection assessment. In line with the storage limitation principle in Article 5(1)(e) of the GDPR, data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Hence, how long personal data shall be kept depends on the purpose for which they were obtained and their nature. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, or scientific or historical research purposes.

Publication of data

The three Models differ in the number of data fields that are publicly available. Model 3 does not display any personal data, whereas Model 2 displays Thin Data + email address for technical and administrative contacts and Model 3 displays Thick Data except the email and phone number of the registrant and the name and postal address of the technical and administrative contacts.

The Commission welcomes the distinction between personal data and other data (about legal persons). The GDPR only applies to personal data of natural persons and therefore does not regulate the processing of the data of legal persons (unless such data also relates to an identified or identifiable natural person).

The Commission notes that the Article 29 Working Party, in its correspondence with ICANN, does not exclude a possible publication of some personal data, as long as this is justified in light of the legitimate purposes pursued with the WHOIS directory

and can be validly based on the legal ground of performance of a contract or the legitimate interests pursued by the controller or by a third party.

It should therefore be assessed in how far publication of the data is necessary for the purposes for which the data is collected by the registrars and processed in the WHOIS directory.

Access by law enforcement

Access to WHOIS data for law enforcement purposes should be lawful and necessary for the performance of a task carried out by a competent authority for law enforcement purposes, in line with the applicable data protection legal framework.

Law enforcement authorities have a clear interest in having access to data in the WHOIS register when it is necessary for their investigation. The data involved could include all current registration information, including email and phone number of registrant, name and postal address of technical and administrative contacts, and billing details as well as historical domain data retained in line with the principle of storage limitation (see above). The access modalities should be designed to ensure that law enforcement can obtain such data within an appropriate time frame for the investigation, through a single portal for data queries. The records should also be searchable in such a way as to allow for cross-referencing of information, e.g. where the same data set was used to register several sites.

The three Models provide different conditions for access by law enforcement authorities to the non-public data in the WHOIS register.

Model 1 provides a self-certification system. If law enforcement agencies (LEAs) are treated like other requestors (and a different treatment of them is not specified in the model), then this procedure means that both LEAs and registries or registrars could be overwhelmed by the large number of necessary applications (according to certain reports, tens of thousands per week for some cyber-crime law-enforcement units).

Furthermore, it is not clear from the description of the model if one self-certification process would be applied across all registries or not. Each and every registry developing its own self-certification process would likely lead to significant inconsistencies in requirements for the requestors who could thus be confronted with very different processes.

The model also lacks a description of how an appeal process against a denial of access would look like – especially, who would decide on it.

Model 2 provides for access to non-public registration data only for a defined set of third-party requestors certified under a formal accreditation/certification program.

The model does not provide details on how the certification/accreditation process should work, in particular who will finally provide certification/accreditation. Neither does it indicate whether one certification/accreditation would be valid for all registries, with a single entry point for requests. An authentication mechanism should take into account the rate of look-ups expected from authorised users and the requirements of confidentiality associated with law enforcement investigations.

The model should give nationally-accredited actors access to all the WHOIS data necessary for the fulfilment of their task, subject to any further requirements (that should be clearly stated in the processing policy of WHOIS data).

As for *private* actors whose interests are not recognised and whose access rights are not regulated in law, it would have to be ensured, for example through the design of the underlying policy and contracts, that access conforms with the requirements of the GDPR, in keeping with objective of maintaining access to WHOIS to the greatest extent possible. This concerns in particular cybersecurity bodies, private sector companies and certain academic researchers, consumer protection bodies, or intellectual property right holders.

States should keep an updated list of public and private entities located in their respective jurisdiction which are allowed to access non-public WHOIS data on the basis of the applicable domestic legislation. The list of public and private entities should be published in a Register which is made accessible to the public.

Model 3 indicates that registries and registrars would only grant access to third-party requestors when required by applicable law and subject to due process requirements, such as when the third-party requestor provides a subpoena or any other order from a court or other judicial tribunal of competent jurisdiction for access to non-public WHOIS data.

Of the three models, this model is most protective from a data protection point of view. The amount of data published is most limited, access to non-public data is subject to legal due process and data is stored for 60 days, instead of 1 or 2 years. However, this does not mean that Model 3 is the desired option; in particular from the WHOIS user point of view, it could make the use of WHOIS, e.g. in criminal investigations, impracticable.

Specific requirements for access by law enforcement to WHOIS data are laid down by national criminal law, which authorities are bound to respect. They are not regulated by the GDPR itself and may differ from EU Member State to Member State (e.g. ex-post validation by judicial authorities or need to obtain a court order). Whether authorities are required to make use of court orders or similar instruments should therefore be left to the law of the investigating state.

Accuracy of data

As stipulated by the EU data protection legal framework and in line with the obligations of contracted parties under their contracts with ICANN, personal data shall be accurate and kept up to date.

Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (retroactive database data correction with regards to the factual data situation found out during the investigation). To comply with the data quality principle, reasonable steps should be taken to ensure the accuracy of any personal data obtained.[2]

Other considerations

There should be sufficient guarantees in place to ensure the implementation of the principle of accountability and purpose limitation. The logging and documentation of the queries and safety of the searches should be made available to the competent oversight authorities for the purposes of verifying the lawfulness of data processing, monitoring and auditing and ensuring proper data integrity and security. Consideration should be given to ensure confidentiality of the requests.

[2] As also recommended in the 2014 Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS), Ch. V.