Council of the European Union

Brussels, 23 October 2018
(OR. en)

13443/18

LIMITE

CYBER 247
CFSP/PESC 975
COPS 379
RELEX 893
JAIEX 141
TELECOM 355
POLMIL 178

'I' ITEM NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee (Part 2)
Subject:	EU Lines To Take on WHOIS policy reform

1. The Horizontal Working Party on Cyber Issues at its meetings of 7 and 28 September 2018 asked the Commission to prepare draft EU lines to take on WHOIS policy reform, in view of the upcoming ICANN63 meeting in Barcelona on 20 - 25 October 2018, which would reflect the current developments and expert discussions on WHOIS.

2. Following these discussions, draft EU lines to take on WHOIS policy reform were prepared by the Commission.

3. The text of the draft was put under silence procedure until 22 October 2018, 10:00 am (Brussels time). Member States raised no objections which made it possible for the Presidency to successfully finalise the draft lines to take as set out in Annex.

4. On this basis, COREPER is invited to endorse the "EU lines to take on WHOIS policy reform" as set out in Annex.

EU LINES TO TAKE ON WHOIS POLICY REFORM

5. The EU and its Member States acknowledge ICANN's central role and responsibility for ensuring the security, stability and resilience of the Internet Domain Name System. As part of this role, ICANN should ensure a functioning WHOIS service, including the collection, retention and publication of accurate information about individual domain names and their registrants, in full respect of EU data protection rules.

- The EU and its Member States support the on-going dialogue between ICANN and the EU data protection authorities to ensure that data processing activities in the context of WHOIS are in line with the EU data protection rules. They acknowledge the efforts made so far by ICANN and the stakeholders' community but stress the necessity to expedite the process and design and implement a stable solution ahead of the expiry date of the ongoing Temporary Specifications in May 2019.

- The EU and its Member States stress that the current situation where access to non-public WHOIS data for public policy objectives is left at the discretion of registries and registrars affects the Member States authorities' ability to obtain legitimate access to non-public WHOIS data necessary to enforce the law online, including in relation to the fight against cybercrime. It may also affect the rights of individuals.

- The EU and its Member States support the development of a unified access model that applies to all registries and registrars and provides a stable, predictable, and workable method for accessing non-public WHOIS data for users with a legitimate interest or other legal basis as provided for in the GDPR, including law enforcement authorities and other public enforcement authorities, including for cybersecurity purposes (e.g. consumer protection and public safety agencies). Such a unified access model should be fully in line with EU data protection rules.

- The EU and its Member States note the concerns raised by law enforcement authorities, cybersecurity organisations and intellectual property rights holders about the negative impact of the limitations of access to WHOIS data on their work. Finding a workable solution for access to non-public WHOIS data should be treated as a matter of priority.

- The EU and its Member States will continue providing input in the WHOIS policy development process via the Government Advisory Committee of ICANN, ensuring that public interests are taken on board, including public policy objectives such as on law enforcement, cybersecurity, consumer protection and the protection of intellectual property.

- In the following, the EU and its Member States set out a number of considerations that they urge ICANN to take into account when designing a model for WHOIS data processing that ensures full compliance with EU data protection rules.

PURPOSE DEFINITION

- 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), should be clearly and explicitly set out in WHOIS policy rules, 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 particular, in Article 13 of the GDPR.

DATA COLLECTION

- In line with the aim to preserve the functioning of the internet domain name system, the obligation to collect WHOIS registration data under ICANN rules should cover what is 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).

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 AND ACCESS TO DATA

- 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). Non-personal data contained in the WHOIS database may thus be published in a publicly accessible way.

- 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, acting in accordance with the applicable legal regime, should have access to data in the WHOIS register when it is necessary for their tasks. 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. The access modalities should be designed to ensure that law enforcement can obtain such data within an appropriate time frame for the investigation, ideally through a single portal for data requests. Requirements on the confidentiality of a request so as not to harm an investigation should be duly considered. 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 domains.

- In order to facilitate access to non-public WHOIS data, States should consider keeping an updated list of public and possibly private entities located in their respective jurisdiction which are considered to have a legitimate interest to access non-public WHOIS data on the basis of the applicable domestic legislation. The list of entities could be made accessible to the public and could allow registries and registrars to take an informed decision while assessing the legitimate interest of an entity to access non-public WHOIS data.

- As for other actors whose access rights are not regulated by law, it would have to be ensured, for example through the design of the underlying policy and contracts, that access to non-public WHOIS data conforms with the requirements of the GDPR, including purpose limitation, in keeping with objective of maintaining access to WHOIS. This concerns in particular cybersecurity bodies, private sector companies and certain academic researchers, consumer protection bodies, or intellectual property right holders.

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.

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. Appropriate safeguards should be provided to ensure confidentiality of the requests.

***

BACKGROUND

The Internet Corporation for Assigned Names and Numbers (ICANN) coordinates the maintenance of the Internet Domain Name System and ensures its secure operation and stability. In this context, ICANN requires domain name operators (registries) and resellers (registrars) to maintain a database with information on each domain name, including technical information and information about the domain name holder (name, email, telephone number and physical address). This information can be retrieved using the "WHOIS" protocol, a query and response protocol that queries the domain name databases and delivers content in a human-readable format. WHOIS data are used for a variety of purposes, including important public policy purposes, such as law enforcement, intellectual property rights protection, consumer safety, and cybersecurity.

The ICANN Board adopted a temporary policy (Temporary Specifications) on 17 May 2018 to ensure compliance of the WHOIS service with GDPR and provide reasonable access for users with a legitimate purpose. This temporary policy will last for a maximum period of 1 year and is to be updated by a multi-stakeholder expedited community-led Policy Development Process" (ePDP) upon the expiry of the Temporary Specifications. In parallel the ICANN Board called on the community to develop by December 2018 a Unified Access Model (UAM) for allowing access to non-public WHOIS data to authenticated users with a legitimate interest consistent with the GDPR.

The Commission and individual Member States have been providing input and feedback primarily via the Governmental Advisory Committee (GAC) of ICANN, including in its last Communiqué of 28 June 2018, and directly, through a number of meetings and correspondence with ICANN.

In its letter of 5 July 2018, the European Data Protection Board (EDPB) also provided a detailed reply to some of the questions raised by ICANN regarding the purpose for and the lawfulness of processing of WHOIS personal data. The EDPB concluded that WHOIS personal data can be made available to third parties with legitimate interest provided that there are appropriate safeguards to ensure "that the disclosure is proportionate and limited to that which is necessary and the other requirements of the GDPR are met, including the provision of clear information to data subjects."