Council of the
European Union

Brussels, 23 January 2018
(OR. en)

5506/18

LIMITE

COSI 10
CYBER 12
TELECOM 19
JAI 36

'I' ITEM NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee (Part 2)
No. prev. doc.:	5274/18, 14762/17
Subject:	Reform of the domain name WHOIS - Draft lines to take - Approval

1. The Council endorsed a Presidency report on the EU law enforcement ("LEA") response in the EU's fight against cybercrime on 7 December 2017[1]. The report outlined four priority issues to be examined further in view of enhancing the EU's capability to respond to cyber threats: (a) criminality on the dark web; (b) joint EU law enforcement response to major cyberattacks; (c) IP address WHOIS reform discussions; and (d) carrier-grade network address translation (CGN) and online crime attribution.

2. Regarding the third priority area (WHOIS reform), the report stated that 'COSI, in cooperation with the Commission, would endorse the draft joint messages and would liaise with other relevant Council preparatory bodies so that a coordinated position of the EU and the Member States on the reform discussions of the WHOIS is approved by the Council and on the messages delivered at ICANN (Internet Corporation for Assigned Names and Numbers)'.

[1] 14762/17

3. At the COSI meeting on 14 December 2017, the Presidency invited delegations to provide written comments, so that lines to take could be developed and ideally agreed in January 2018 to ensure that EU law enforcement needs are taken into account in the WHOIS reform discussion.

4. On 12 January 2018, ICANN published a proposal for three potential interim compliance models with ICANN's agreement and policies in relation to the EU's General Data Protection Regulation. It requested feedback by 29 January 2018 through its Governmental Advisory Committee (GAC). All EU Member States and the Commission are represented in the Governmental Advisory Committee. ICANN intends to decide on and publish a single compliance model by 31 January 2018.

5. In this respect, on 19 January 2018 draft lines to take on the 'reform of the domain name WHOIS database'[2] were presented at a joint meeting of the Horizontal Working Party on Cyber Issues and the COSI Support Group.

6. The revised lines to take, resulting from the comments from delegations and confirmed under written consultation on 23 January 2018, are found in the Annex to this Note.

7. The present lines to take are intended to ensure that law enforcement needs are taken into account in the WHOIS reform process in ICANN. They are without prejudice to further analysis of other relevant issues in this context, such as data protection.

8. In view of the above,

   1/ Coreper is invited to endorse the draft lines to take on the minimum requirements for LEA access to a layered-access WHOIS system, as set out in the Annex;

[2] 5274/18

2/ Coreper invites:

a/ the Commission to present a submission, on behalf of the Union, to the Governmental Advisory Committee (GAC) of ICANN with a view to informing the GAC's feedback to ICANN on a compliance model with ICANN's agreement and policies, alongside the lines to take set out in the Annex; and

b/ the Member States to uphold these lines to take in that context.

ANNEX

Reform of the domain name WHOIS database

Draft lines to take on minimum requirements for LEA access to a layered-access WHOIS system

The objective of this line to take is to ensure that the EU speaks with one voice at the upcoming ICANN discussions on the reform of the WHOIS database. The lines also implement the recent EU Council Conclusions on Building Strong Cyber Security which recognise the importance of "ensuring swiftly accessible and accurate WHOIS databases of IP-addresses and domain names so that law enforcement capabilities and public interests are safeguarded."[1]

These lines to take are in line with the European Data Protection legal framework, namely the General Data Protection Regulation (Regulation (EU) 2016/679 - GDPR) and the Police Directive (Directive (EU) 2016/680).

2.1. Basic principles

- The different legitimate purposes for which processing of registration data takes place should be clearly and explicitly set out in the policy rules that apply to such processing, from collection to storage and access of data.

- Processing of WHOIS data for law enforcement purposes, e.g. investigating and countering serious crime, fraud, consumer deception, intellectual property violations, and other law violations, constitutes a legitimate interest for processing of personal data. The processing of personal data shall be lawful and necessary for the performance of a task carried out by a competent authority for law enforcement purposes, in line with applicable data protection legal framework.

- These purposes should therefore cover the legitimate need for law enforcement access to WHOIS data[2] to sustain public interests such as cybersecurity; the stability, reliability and resilience of the network; preventing and fighting crime; protecting intellectual property rights, copyright and consumer rights; and other rights recognised in the domestic legal order.

- 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.

---

1 Council of the European Union, Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defense: Building strong cybersecurity for the EU. Available at http://www.consilium.europa.eu/media/31666/st14435en17.pdf.

2 As recognised by ICANN's Bylaws (ICANN Bylaws Article One, Section 1.1; Section 1.2 (a) Commitments and Core Values; Registration Directory Services Review, §4.6(e)

2.2. Necessary data elements

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

- This includes all current registration information available, public and non-public, personal and non-personal, including email and phone number of registrant, name and postal address of technical and administrative contacts, and billing details, which should continue to be collected by registries and registrars.

2.3. Accreditation system

- Accreditation of Law Enforcement and Public Safety agencies which have a legitimate need to access WHOIS data for the purposes mentioned in 2.1, should be carried out at national level instead of being carried out centrally, e.g. at European or global level.

- The accreditation system should ideally guarantee access for other relevant actors, based on the specific purposes defined pursuant to point 2.1 for processing, including accessing of WHOIS data, comprising non-public elements. This concerns in particular cybersecurity authorities, private sector companies and academic researchers, consumer protection authorities, 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 relevant domestic legislation. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. Therefore, the list of the public and private entities should be published in a Register which is made accessible to the public.

- This system could be based on the certification programme described by ICANN in relation to the second model of the interim GDPR compliant WHOIS system[3], provided that programme can accommodate the minimum requirements described in this document. The set of requirements for the issuance of certificates should be clear and transparent.

[3] See p. 7 of https://www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf

2.4. Authentication of access

- Authentication mechanisms should be compatible with the rate of look-ups expected from authorised users.

- Nationally-accredited requestors (with a legitimate need to access non-public WHOIS data based on domestic law) should be provided with the necessary level of access to requested WHOIS data through a unique set of credentials.

2.5. Access policy, data location and confidentiality

- Access WHOIS data needs to be maintained regardless of location of storage. This could be achieved in practice through a centralised federated access system, e.g. hosted by ICANN.

- Nationally-accredited entities with a legitimate need to access non-public WHOIS data on the basis of domestic law should have permanent access to WHOIS data on a query basis. Access should not be based on individualised requests justifying the purpose for access, specific data elements sought, nor should it be required to provide a subpoena or any other order from a court or other judicial authority to gain access to non-public WHOIS data.[4]

- 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.

- To ensure confidentiality of the requests, WHOIS data look-ups by nationally-accredited and authenticated actors should be anonymised, possibly through a system of hashes, be logged by them for audit purposes. Such WHOIS data look-ups should not be limited in number or time.

[4] Previously covered under section 2.3

2.6. Accuracy and validity 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.

2.7. Data Retention and Record of historical WHOIS data

- In order to ensure the availability of historical WHOIS data, the WHOIS system model should allow access to historical domain data retrospectively. Historical domain and IP ownership information[5] is necessary for the success of investigation by LEA and other parties, and thus an adequate retention policy for historical data should be implemented.

- The data retention period for the different categories of personal data should be based on individual business needs and a proper data protection assessment. A judgement must be made about: the current and future value of the information; the costs, risks and liabilities associated with retaining the data; and the ease or difficulty of making sure it remains accurate and up to date. How long personal data shall be kept depends on the purpose for which they were obtained and their nature.

- Such 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.

- In line with the storage limitation principle, 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; 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.

---

5 For example as offered by Domaintools.