Building Block d) *(Acceptable Use Policy[1] - Requestor)*

Staff support team comment: d) From use case template: EPDP Team to further define / clarify who and how auditing is expected to be carried out.

The EPDP Team recommends that the following requirements are applicable to the requestor and must be confirmed & enforced by [TBC]:

a) Must only request data from the current RDS data set (no data about the domain name registration's history);
b) Must provide representations with each unique request for data of its corresponding purpose and legal basis for their processing which will be subject to auditing (no bulk access);
c) Must only use the data for the purpose requested;
d) Must handle the data subject's personal data in compliance with data protection laws such as GDPR;
e) Must provide representations about use of requested data which will be subject to auditing;
f) [Other]

[Additional requirements in the case of the following purpose [state purpose] are:
TBC based on review of use cases]

Comments / concerns / questions to be considered in relation to building block d):

- *Re. b), consider including reference to RAA definition of bulk access (Section 3.3.6).*
- *Re. c), further specificity would need to be provided. Consider that GDPR Art 42/43 Certification and the flipside of De-accreditation and Decertification as a mechanism to ensure the fidelity of safeguards.*
- *Re. c), consider updating as follows and striking e) (""Must represent that requestor will only use the data for the purpose requested").*
- *Re. d), is this necessary as compliance with the law is a given?*
- *Re. d), Consider changing "such as GDPR" to "including the GDPR".*

Building Block h) *(Acceptable Use Policy[2] - entity disclosing the data)*

Staff support team comment:
Re. d), Must all requests be logged? What information must be logged? Who would be able to access the logs? EPDP Team may want to consider the guidance the European Data Protection Board provided on this issue in its 5 July 2018 letter. ("The EDPB considers that, unless there is an explicit prohibition in national law, appropriate logging mechanisms should be in place to log

[1] Charter questions c1-7
[2] Charter questions c1-7

any access to nonpublic personal data processed in the context of WHOIS. In this context, such logging is considered required as part of the security obligation of controllers (article 32), as well as the obligation and in order to be able to demonstrate compliance with the GDPR (accountability) (article 5(2))… It is up to ICANN and other controllers participating in the WHOIS system to ensure that logging information is not disclosed to unauthorized entities, in particular with a view of not jeopardizing legitimate law enforcement activities.")

Re. e), Does this imply that the data subject is informed every time a balancing test is carried out with respect to his/her data?

The EPDP Team recommends that the following requirements are applicable to the entity disclosing the data and must be confirmed & enforced by [TBC]:

a) Must only supply the necessary data requested by the requestor;
b) Must return current data in response to a request;
c) Must process data in compliance with data protection laws such as GDPR;
d) Must log requests;
e) Where applicable, must define and perform a balancing test before processing the data. The data subject should be able to challenge –with proper substantiation- the balancing test with rights to object and to erasure;
f) Must disclose to the Registered Name Holder (data subject), on reasonable request, confirmation of the processing of personal data relating to them, per relevant data protection laws such as GDPR;
g) Any system designed for disclosing of non-public registration data to Law Enforcement Authorities must include a mechanism for implementing the need for confidentiality for ongoing investigations.

Comments / concerns / questions to be considered in relation to building block h):

- *Can this topic be addressed without confirming who the entity/entities disclosing the data is?*
- *How can these requirements be enforced?*
- *Re. e), consider that yes, data subjects should be informed, with the exception of sensitive LEA investigations. Consider generalizing this section as in its current form it may be too GDPR centric.*
- *Consider adding h) "h) Must provide [non personal] non-public data for data subjects that are legal persons or otherwise not subject to data protection laws."*
- *Consider having the policy should acknowledge that the SSAD be built to accommodate accredited groups, and that there should be a framework for recognizing groups that are accredited. The EDPB could then review this overall concept but may not need to have a role to review each accredited group?*

From SSAD Worksheet: Acceptable Use Policy

Objective: Define the policy requirements around:

1. How should a code of conduct (if any) be developed, continuously evolve and be enforced?
2. If ICANN and its contracted parties develop a code of conduct for third parties with legitimate interest, what features and needs should be considered?
3. Are there additional data flows that must be documented outside of what was documented in Phase 1?

Can a Code of Conduct model compliment or be used with what is implemented from EPDP-Phase 1 Recommendation #18?

Related mind map questions:

P1-Charter-c
c1) What rules/policies will govern users' access to the data?
c2) What rules/policies will govern users' use of the data once accessed?
c3) Who will be responsible for establishing and enforcing these rules/policies?
c4) What, if any, sanctions or penalties will a user face for abusing the data, including future restrictions on access or compensation to data subjects whose data has been abused in addition to any sanctions already provided in applicable law?
c5) What kinds of insights will Contracted Parties have into what data is accessed and how it is used?
c6) What rights do data subjects have in ascertaining when and how their data is accessed and used?
c7) How can a third party access model accommodate differing requirements for data subject notification of data disclosure?

Materials to review:

Description	Link	Required because
GDPR Article 40, Code of Conduct	https://gdpr-info.eu/art-40-gdpr/	

Art. 29 Working Party Letter to ICANN 11 April 2018	https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf	
Bird & Bird - Code of Conduct and Certification Reference Material (May 2017)	https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/43--guide-to-the-gdpr--codes-of-conduct-and-certifications.pdf?la=en	
Example: Cloud Providers Code of Conduct (CISPE) (January 2017)	https://cispe.cloud/code-of-conduct/	
Example: Cloud Providers Code of Conduct (EU Cloud) (November 2018)	https://eucoc.cloud/en/contact/request-the-eu-cloud-code-of-conduct.html	

Related EPDP Phase 1 Implementation: None.

Tasks:

- Determine full list of policy questions and deliberate each
- Determine possible solutions or proposed recommendation, if any
- Confirm all charter questions have been addressed and documented