**Automation Use Cases Legal Questions**

The EPDP team is deliberating on a set of use cases for potential automation of the decision to disclose non-public registrant data (attached as Exhibit 1).  This automation under consideration would occur within the hybrid model for disclosure, which consists of a Central Gateway for the intake of requests by accredited users with the ultimate decision to disclose resting with Contracted Parties (who possess the underlying non-public registration data). Under the proposed automation use cases, the Central Gateway would make an automated recommendation on disclosure, which is then communicated to the relevant Contracted Party. The Contracted Party may then choose to follow that decision and disclose the data (see “Assumptions” in Exhibit 1 for further details).

1. In light of the advice previously provided in the memos on Question 1&2 (Liability) and Question 3 (Automation), **please provide the following analysis for each use case in Exhibit 1**:
2. Please describe the risk of liability for the Central Gateway and Contracted Parties related to automating this recommendation, and to automating the decision to disclose personal information to a third-party. If there is additional information required to assess the risk, please note the additional information needed.
3. Is the decision to disclose personal information to a third-party a decision “which produces legal effects concerning [the data subject] or similarly significantly affects him or her” within the scope of Article 22?
4. Are there additional measures or safeguards that would mitigate the risk of liability?
5. Does automated decision-making performed in this manner impact your analysis on the roles/liability of the parties described in the Question 1&2 memo (e.g., Contracted Parties remain controllers with liability where “disclosure takes place in an automated fashion, without any manual intervention.” 1.1.4).
6. Consider an alternative scenario (see “Assumptions” in Exhibit 2 for further details) where the Central Gateway has the contractual ability to require the Contracted Parties to provide the data to the Central Gateway (i.e. without the Contracted Party being able to review the request). In this alternative, please consider both a scenario where the Central Gateway obtains data from the Contracted Party and evaluates the data as part of its decision making, as well as a scenario where the Central Gateway makes a decision without processing the personal data (i.e. the decision is based solely on information the Central Gateway knows about the requestor and the assertions made in the request). One example of the latter scenario would be automated disclosure to the verified owner of the trademark MICROSOFT, which requests registration data for microsoft-login.com, alleging trademark infringement and asserting its intent to process the data for the establishment, exercise or defense of legal claims.
	1. How do these alternative scenarios impact the analysis provided in Questions 1 through 4 above?
	2. Which scenario involves the least risk of liability for Contracted Parties?

In responding to this, please state your assumptions regarding the respective roles of ICANN and contracted parties, including a scenario where the Centralized Gateway has outsourced decision making to an independent legal service provider.

1. Additional automation clarifications
2. If the decision to disclose personal data to a third party is automated, in what manner must the Controller(s) provide the registrant with information concerning the possibility of automated decision-making in processing of his or her personal information? How should this information be communicated to the registrant, and what information pertaining to the automated decision-making must be communicated to the registrant in order to ensure fair and transparent processing pursuant to Article 13?
3. Does the provision of the information in the answer to question C.1 above by the Controller(s) affect the registrant’s right to obtain confirmation as to whether or not automated decision-making to disclose their personal information to a third-party has taken place? Does it affect the registrant’s right to obtain associated meaningful information as per Article 15.1(h)?
4. Does the manner in which the decision making is performed above impact the way in which this information must be provided?
5. What role does proximate cause play in determining whether a decision to disclose produces a legal or similarly significant effect (i.e. how related must the decision to disclose a registrant’s personal data be to the ultimate legal or similarly significant effect of personal data processing)? Please describe the risk of liability to the Central Gateway or Contracted Party if, after receiving personal data, the requestor engages in its own processing which has a legal or similarly significant effect.
6. In Section 1.12 in the previous memo on Automation, Bird & Bird stated:

It may also be possible to structure the SSAD so that it does not involve "*a decision basedsolely on automated processing".* To expand, rather than the SSAD requesting information from requesters and evaluating if the relevant criteria for release of non-public registration data are met, the SSAD could publish the categories of requests which will be accepted and ask requestors to confirm that they meet the relevant criteria. In this case, there would be no automated processing leading to a decision to release the data. The SSAD could ask requesters to provide additional information about the nature of their request for audit purposes – but it would not be used to evaluate the request itself.

C(i) publishing the categories of requests that will be approved and (ii) requiring a requestor to manually select the applicable category and confirm that they meet the criteria for that category of requests would make the decision to disclose “not automated”?

**Exhibit 1**

*DISCLAIMER:* *These use cases were submitted by Mark Svancarek (BC) for discussion by the EPDP Team. These do not represent EPDP Team consensus. Further deliberation is necessary to determine which, if any, of these use cases have the support of the EPDP Team to be included in the Final Report as additional use cases that would support automated disclosure decisions.*

Use Cases That Support Automated Disclosure Decisions – [V2.10]

Assumptions:

1. All requestors have been accredited by Accreditation Authority and all requestors are individually authenticated by the Gateway.
2. All requests are syntactically correct and complete, including any/all required Authorization Assertions.
3. The Authorization Provider has access to the data required to make the decision, such as access to the Public RDS/WHOIS data collected per Phase 1 Policy, or various flags indicating prior disclosure.
4. In addition to other attestations, a requestor shall assert whether data disclosed in response to a particular request is intended to be used in a way that has legal or similarly significant effects on the data subjects. If the intended use for the data changes after disclosure to one intended to have legal or similarly significant effects on the data subjects, the data shall be discarded and requested again under new assertions.
5. The Gateway may have enough information to make an informed suggestion to a CP regarding the CP’s processing. CPs with enough confidence in the Gateway may choose to automate based on the Gateway's recommendation.
6. CPs shall provide feedback about the quality of past recommendations to the Gateway in order to improve the recommendation of future recommendations.
7. The Gateway can automate a limited subset of recommendations based on the request alone. Theoretically, the Gateway could request the nonpublic RDS data to make a more informed recommendation, but such cases would require the Gateway Operator to be a data controller, not just for the data of requestors, but for registrant data as well. The use cases below should not require the Gateway to request such nonpublic data.
8. As more legal certainty is acquired, additional use cases may be added to this list.
9. The algorithms generating the recommendations of the Gateway shall be published and subject to ongoing review to ensure consistency and fairness.

Use Cases:

1. **LEA in same jurisdiction as CP**
	1. Examples
		1. Law Enforcement Agency from Jurisdiction A requests Registrant RDS data from a Registrar also in Jurisdiction A
		2. Competent DPA requests data in response to a Data Subject complaint that their data is being misused in violation of the GDPR
	2. For the Gateway to make a good recommendation, access to the City field may be required; see below
2. **Request for City Field (only)**
	1. Examples
		1. Requestor submits a request for the City field in order to ascertain which specific jurisdiction to make a legal claim, or
		2. Requestor submits a request for the City field for the purpose of statistical research or similar non-legal purpose
	2. In each example, our Phase 1 policy suggests that the requestor should not join the City field data with any other data held concerning the same data subject.
		1. In Example 2a(i), it is safest if the City field is requested first for purposes of determining jurisdiction, then discarded before requesting the remainder of the data required for the legal claim.
3. **Registration record contains no personal data and has already been disclosed**
	1. Once registration data has been determined to contain no personal data (e.g. as a result of a previous disclosure), it can be flagged for automatic disclosure in future requests.
		1. The flag remains valid so long as none of the data fields have changed.
	2. The Gateway shall determine whether any data fields have changed by inspecting the Public RDS/WHOIS data.
	3. The flag could be stored at either the CP and/or in the Gateway.
	4. A registrar could optionally implement a system to flag such a domain for automation when the data is collected, to enable later automation.
	5. NOTE: Some TLDs are not expected to contain any personal data, and this can streamline processing.
		1. See .BANK, .INSURE, .MUSEUM, and others
		2. There may be other TLDs whose registries enforce policies requiring disclosure, even for personal data, which may streamline processing
		3. There should be a verification element included in the registry policies to detect registrants who circumvent the registry policy requirement
4. **Registration record has already been disclosed under the same authorization assertions to a requestor of the same type**
	1. Once registration data has been disclosed, it can be flagged for automatic disclosure in future requests if
		1. The same authorization assertions are used, and
		2. The requestor is of an equivalent type to the previous one, and
		3. None of the contact data fields have changed
		4. Example:
			1. Requestor is an accredited cybersecurity entity requesting to investigate phishing, and the data was already disclosed to a different accredited cybersecurity entity investigating phishing
	2. Gateway can determine whether any data fields have changed by inspecting the Public RDS/WHOIS data
	3. The flag includes details of the previous assertions and previous disclosed-to entity type
	4. The flag could be stored at either the CP and/or in the Gateway.
	5. A registrar could optionally implement a system to flag such a domain for automation when the data is collected, to enable later automation
	6. NOTE: If a record is known to contain patently false information as a result of a previous review, and has already been disclosed, a CP could elect to flag it as such for future processing
5. **“Clear cut” TM claim**
	1. Trademark Owner of "<Example Trademark>" submits a request for RDS data supporting a trademark infringement and justifies its need/necessity to get access to Registrant RDS data based on the intended use of the data.
		1. The trademark exists in the Trademark Clearinghouse (TMCH)
		2. The trademark must be “live” (not just applied for, rejected or expired)
	2. TM owner has proved it has "agency" to request this data
		1. The owner of the TM, or
		2. Entity acting on behalf of the owner
	3. Limits
		1. The trademark string is of sufficient length/complexity that collisions with non-trademark strings is very unlikely (e.g. “microsoft”)
		2. The domain name non-public registration data requested is identical with the trademark, or the trademark is a prefix, infix or suffix of the domain name
		3. Automation would not work for figurative marks or where the domain name is allegedly confusingly similar to the trademark.
		4. Since pattern-matching for evaluation of trademark infringement may be complex and vary between locales, the publication of algorithms in Assumption IX is particularly relevant to this use case.
		5. Trademark investigations take many forms. Sometimes data is needed simply for contacting a name holder; sometimes data is needed to file a claim. Since data may be requested for purposes other than those having legal or similarly significant effects on the data subjects, the assertion from Assumption IV is particularly relevant to this use case.
6. **Request for data from ICANN Compliance**
	1. In order to investigate *[something that is allowed and specified in ICANN's role as controller]* ICANN requests RDS data for a domain name under investigation, such as auditing, validity of name holder, compliance with other laws, (i.e. accuracy under Art. 5 GDPR)
	2. ICANN must agree to be a controller for the purpose of this processing.
	3. This use case should be revisited once examples of “*something that is allowed and specified in ICANN's role as controller*”have been identified.
7. **Identify infrastructure involved in botnets, malware, phishing, and consumer fraud**
	1. Requestor is accredited as a cybersecurity professional and has agreed to comply with specific cybersecurity codes of conduct, if applicable.
		1. Not everyone can simply assert that they are such a professional.
	2. Requestor represents that it has investigated and confirmed that the domain name is being used as part of a criminal infrastructure.
		1. Direct evidence can also be included in the request - based on the Request contents building block.
	3. Cybersecurity investigations take many forms. Usually data is needed simply for identifying infrastructure, with no expectation that legal action can or will be taken; however, it is possible that data might be submitted to LEA to take legal action. As a result, the assertion from Assumption IV is particularly relevant to this use case.
8. **Request for data from a UDRP/USR Provider.**
	1. UDRP or URS Provider has received a UDRP or URS filing for the domain name.
	2. The Registrar must provide the UDRP or URS Provider with the information requested in the verification request, per section 4(b) of the Rules for Uniform Domain Name Dispute Resolution Policy. (<https://www.icann.org/resources/pages/udrp-rules-2015-03-11-en>)

**Exhibit 2**

Assumptions:

1. All requestors have been accredited by Accreditation Authority and all requestors are individually authenticated by the Gateway.
2. All requests are syntactically correct and complete, including any/all required Authorization Assertions.
3. The Authorization Provider has access to all data required to make the decision, including access to all Non-Public RDS/WHOIS data collected per Phase 1 Policy, and various flags indicating prior disclosure.
4. In addition to other attestations, a requestor shall assert whether data disclosed in response to a particular request is intended to be used in a way that has legal or similarly significant effects on the data subjects. If the intended use for the data changes after disclosure to one intended to have legal or similarly significant effects on the data subjects, the data shall be discarded and requested again under new assertions.
5. The Gateway will have enough information to make an informed decision to a CP regarding the CP’s processing; such information shall include the Gateway’s unencumbered access to the Non-Public RDS data held by the CP. CPs are required to automate their response with all requested data back to the Gateway based on the Gateway's decision.