Bird & Bird LLP
12 New Fetter Lane
London EC4A 1JP
United Kingdom
Tel +44 (0) 20 7415 6000
Fax +44 (0) 20 7415 6111
DX 119 London
twobirds.com

Bird & Bird

DRAFT MEMORANDUM

To: Internet Corporation for Assigned Names and Numbers (ICANN), EPDP Team
From: Ruth Boardman & Katerina Tassi, Bird & Bird LLP
Date: 23 April 2020
Subject: Advice on use cases re automation in the context of disclosure of non-public registrant data

---

EXECUTIVE SUMMARY

This document examines the scenarios and use cases presented by the EPDP Team in relation to automated decisions for disclosure of non-public registrant data. It identifies the cases of fully automated decisions that would fall under the scope of Art. 22 GDPR, challenges associated with Art. 22 and available alternatives. The document further suggests data protection safeguards and examines transparency considerations in the SSAD context. Finally, it examines the status of the parties under each scenario and the associated risk of liability.

Art. 22 decisions and alternatives

Art. 22 GDPR applies to fully automated decisions which produce legal or similarly significant effects. Art. 22 decisions are only allowed in limited cases, which are not likely to apply to the SSAD context.

Fully automated decisions will only be allowed if they:

(a) do not include the processing of personal data;
(b) do not produce legal or similarly significant effects;
(c) are authorised by applicable EU or Member State law which lays down suitable measures to protect individuals; or
(d) are covered by a national derogation from Art. 22 (for example, for the purpose of detection of criminal offences).

In all other cases, there needs to be meaningful human involvement in the decision making process.

Do Art. 22 criteria apply to SSAD?

(a) Solely automated processing: For Art. 22 to apply, there needs to be *some* processing of personal data, but there is no requirement that *only* personal data is processed for the decision. The decision examined here will in most cases involve the processing of personal data – this will be the case irrespective of whether or not the Central Gateway has access to the requested data and takes account of such data in the decision making.

Apart from Scenario 1.a where the SSAD would only issue an automated recommendation, all other scenarios would include a decision (to disclose registrant data to third parties) based solely on automated processing.

(b) Legal or similarly significant effect: the term is not defined in the GDPR; however, it indicates an elevated threshold. Whether or not the disclosure of registrant data has such an effect, will depend on the circumstances of the request: the document assesses the nature of the effects of disclosure under each use case. We have given clear yes and no answers where possible: some use cases would benefit from further discussion. The role of proximate cause in determining the effects of a decision has not been examined by courts or supervisory authorities. There is some discussion in German literature; however, given the lack of wider discussion, the views of supervisory authorities on this topic could be useful, as this may permit automation of the SSAD on the basis that the Central Gateway/ CPs are only taking a preparatory decision.

Safeguards

A list of suggested data protection safeguards is set out in Appendix 2 of this document. This includes among other things: engaging with supervisory authorities, clearly scoping each use case and establishing a legal basis, imposing appropriate terms of disclosure on the Requestor, implementing appropriate security measures, taking measures to comply with the accountability principle, establishing policies for satisfying individuals' rights, and entering into appropriate data protection clauses with processors.

Transparency

The manner of providing information is not affected by the existence of automated decision making; but the content of the information is.

- The information will typically be provided through the privacy notice; given the importance of the SSAD in the Domain Name system, it would be appropriate to present it in a prominent manner.
- It would be most efficient for registrars to provide the relevant information (given their direct relationship with registrants), irrespective of whether not they are considered controllers in the SSAD context. If they are not controllers, but provide the information on behalf of the controller, this should be made clear to registrants.
- In terms of the content, for Art. 22 decisions only, the notice must also include information about: the existence of automated decision, the logic involved and the significance and envisaged consequences of the processing.
- The elements of Art. 15 GDPR (right of access) need to be provided on request even if they have already been included in the notice.
- The right of access requires controllers to provide information on the recipients to whom the data "*have been* or will be disclosed": this indicates that, absent applicable exemptions, registrants exercising their right of access must be informed about disclosures of their data to third parties.

Status of parties

(a) Under Scenario 1, the ultimate decision to disclose registrant data rests with the CPs. The analysis carried out in the Liability memo would also apply here and most likely CPs would be considered by supervisory authorities as joint controllers along with ICANN.

(b) Under Scenario 2, the situation is less clear. Depending on whether a macro- or micro-level approach is adopted, the CPs may be found to be (joint) controllers for the automated decision making and the disclosure of data to Requestors or merely for the disclosure of data to the Central Gateway. We think the second option (controllers just for the disclosure of data to the Central Gateway) is the better analysis, but the point is not clear. The outsourcing of the decision making to an independent legal service provider would be unlikely to alter the above position.

In both scenarios, it would not be plausible to argue that CPs are processors.

Liability of CPs is examined in respect of:

(a) status of CPs: where CPs are joint controllers, it is important to clearly allocate tasks and responsibilities by means of an agreement;

(b) type of liability:

- Liability towards individuals: the rule is joint and several liability and CPs can be held liable for the entire damage caused by processing they are involved in, irrespective of their status. They can only avoid this by demonstrating that they were not in any way involved in the event giving rise to the damage. Otherwise, they have the right to claim back from the other controllers the part of compensation corresponding to their responsibility.
- Liability to supervisory authorities: joint and several liability is less clear here and there is scope to argue that enforcement action should be imposed based on the "degree of responsibility" of the party.

In terms of risk, Scenario 2 seems to present lower risk of liability both in respect of compensation to individuals and of enforcement action by supervisory authorities.

Background

ICANN has been examining the establishment of a Unified Access Model (UAM), for the disclosure of registrant personal data to third parties following legitimate requests[1]. ICANN has been examining the possibility of automating the assessment of disclosure requests and the decision on disclosure of registrant data to third parties.

We have previously advised ICANN on (i) the status of contracted parties as controllers or processors and the safeguards to be considered in the context of a System for Standardised Access/ Disclosure ("SSAD") (Liability memo), and (ii) GDPR considerations in relation to automated assessment of requests for disclosure and the applicability of Art. 22 GDPR (Automation memo).

We have been asked additional questions, outlined below, which we have been asked to consider in relation to the following two scenarios:

1. Under the first scenario, the automation would be carried out within a Central Gateway tasked with receiving requests from accredited users. The Central Gateway would make an automated recommendation on whether or not the requested data should be disclosed whilst the ultimate decision of disclosing data would rest with the Contracted Parties, which could either follow the recommendation or not (**Scenario 1.a.**). Contracted Parties with enough confidence in the Gateway may choose to automate the decision to disclose the data (**Scenario 1.b.**).

2. Under the second scenario, the decision to disclose the registrant data would be taken by the Central Gateway without the Contracted Party being able to review the request. The Central Gateway would take this decision either (i) after obtaining the relevant data from the Contracted Party and evaluating the data as part of its decision-making (**Scenario 2.a.**), or (ii) without obtaining the registrant data (in which case, the decision would be based solely on information about the Requestor and the assertions made in the request) (**Scenario 2.b.**). One example given of the latter scenario would be automated disclosure of registration data for microsoft-login.com to the verified owner of the trademark MICROSOFT, in response to a request alleging trademark infringement and asserting intent to process the data for the establishment, exercise or defence of legal claims.

We have been asked to assume that each scenario would be subject to a set of safeguards which are included in this memo as Appendix 1.

[1] This memo has been drafted taking into account the document: "Exploring Unified Access Model for gTLD Registration Data" issued on 25 October 2019.

Questions

A. Use cases under Scenario 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:

1. Please describe the risk of liability for the Central Gateway and Contracted Parties ("**CPs**") 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.

2. 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?

3. Are there additional measures or safeguards that would mitigate the risk of liability?

4. 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).

B. Use cases under Scenario 2:
In the second –alternative- scenario, where the Central Gateway has the contractual ability to require the Contracted Parties to provide the data to the Central Gateway:

1. How do the 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.

C. Additional automation clarifications

1. 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?

2. 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)?

3. Does the manner in which the decision making is performed above impact the

way in which this information must be provided?

4. 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.

5. 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 based solely 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.

Could you please elaborate on how (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"?

Structure of the advice

This memorandum is divided into the following sections:

1. **Introduction and legal context**: this sets out the legal provisions and main considerations on the basis of which we have drafted our advice. The legal analysis of the use cases depends on whether or not the associated decision-making process falls under Art. 22(1) GDPR[2] ("Art. 22 processing"). Art. 22 processing is, in principle, prohibited and only allowed under specific circumstances. As a result, we examine this question first, as it impacts the overall lawfulness of the decision-making process.

2. **Solely automated decision making**: In this section we examine the scenarios set out in the Background section and we analyse whether in each case, the automated recommendation and/or decision to disclose registrant data would be considered "solely automated decision making" in the sense of Art. 22 GDPR. This section relates to question A.1 above.

[2] Article 22(1) GDPR: "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects him or her".

3. **Legal or similarly significant effect**: Here, we examine whether the decision to disclose personal data in each use case would have legal or similarly significant effects. We also consider the role of proximate cause in determining a legal or similarly significant effect. This section corresponds to questions A.2 and C.4.

4. **Alternatives to Art. 22 GDPR:** We then proceed with examining alternatives and exemptions from Art. 22 GDPR which may be established under national legislation, by virtue of Art. 23 GDPR. This section relates to questions A.3.

5. **Additional safeguards and transparency considerations**: In this section we examine the safeguards to be considered in the SSAD context and we review the transparency queries posed by the EPDP team. This section along with Appendix 2 corresponds to questions A.3, C.1-3 and C.5.

6. **Status of parties and liability**: In this section, we assess whether any of the scenarios presented by the EPDP would alter our previous assessment regarding the status of CPs as controllers or processors. On this basis, we examine the risk of liability for CPs and reflect on the scenario which would entail the least liability for CPs. This section addresses questions A.1, A.4, B.1 and B.2.

Appendix 1: sets out the Safeguards and Use Cases presented by the EPDP team.

Appendix 2: sets out Safeguards suggested by us.

Analysis

1. Introduction and Legal context

1.1. The GDPR sets out a general prohibition of automated decision making falling under Art. 22. This can only be lifted in very limited circumstances which are not likely to apply in the SSAD context. As noted above and as explained in the Automation memo, therefore, it is fundamental to establish which of the scenarios would fall under the scope of Art. 22 GDPR.

1.2. As a preliminary point, the EPDP team should be aware that the structure and content of Art. 22 GDPR is unclear; this is apparent from commentary around its application[3]. The Article 29 Working party has issued guidelines on automated decision making and profiling ("WP251")[4] which have been approved and adopted by its successor, the European Data Protection Board ("EDPB"); however, ambiguity persists. Although similar provisions on automated decision making were included

[3] By way of example: Bryce Goodman and Seth Flaxman, '*European Union regulations on algorithmic decision-making and a "right to explanation*" ' (ICML Workshop on Human Interpretability in Machine Learning (WHI 2016), New York, NY, 2016); Dimitra Kamarinou, Christopher Millard and Jatinder Singh, '*Machine Learning with Personal Data*' (2016) Queen Mary School of Law Legal Studies Research Paper No. 247/2016; Sandra Wachter, Brent Mittelstadt and Luciano Floridi, '*Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*' (2017) 7 International Data Privacy Law 76; Lilian Edwards and Michael Veale, '*Slave to the Algorithm? Why a "Right to an Explanation" is Probably Not the Remedy You Are Looking For*' (2017) 16 Duke Law and Technology Review 18.

[4] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 ("WP251").

in the GDPR's predecessor, the Data Protection Directive[5], such provisions have not been the subject of enforcement actions, relevant case law or extensive regulatory guidance. The lack of clarity in the legal drafting, along with the absence of relevant case law creates uncertainty over how Art. 22 is to be interpreted and implemented.

1.3. By way of reminder, Article 22(1) GDPR applies to:

(a) "a decision based solely on automated processing, including profiling"

(b) "which produces legal effects concerning ..[the individual] or [which] similarly significantly affects .. [the individual]".

The first criterion is examined in Section 2 below. The second criterion has been reviewed in the Automation memo and is also analysed in more detail in Section 3.

1.4. When a decision meets the above criteria, then it will be allowed only if:

(a) necessary for the performance of a contract between a controller and the individual;
(b) authorised by applicable EU or Member State law which lays down suitable measures to safeguard the individual; or
(c) based on the individual's explicit consent.

1.5. Conditions (a) and (c) will not be applicable to the SSAD context. Condition (b) might possibly be relevant to specific use cases; however, unless an EU law applied to the decision making, this would require consideration of national legislation, adding complexity and possibly fragmenting the SSAD[6]. Also, additional considerations might need to be taken into account where the decision is taken by or on behalf of the Centralized Gateway and where the relevant legal provision only applies to the Contracted Party.

1.6. The GDPR (Art. 23) also allows EU or Member State law to restrict the application of Art. 22 GDPR, among other provisions, for example, for the prevention, detection, investigation and prosecution of criminal offences, or the enforcement of civil law claims. Although this could potentially assist, it would raise the same complexities as highlighted in section 1.5 above.

1.7. On the basis of the above, solely automated decisions can take place in the SSAD context where:

(a) The GDPR is not applicable to the disclosure (because the requested data is not personal data);
(b) The decision does not have a legal or similarly significant effect;
(c) A Member State derogation applies under Art. 23 GDPR; or
(d) An applicable Member State law authorizes the decision, under Art. 22(2)(b) GDPR.

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Data Protection Directive").
[6] For more detailed analysis, see Automation Memo, Appendix: exemptions from Article 22(1) GDPR.

In cases where none of the above conditions apply, there must be meaningful human involvement in the decision making process.

2. Solely automated decision making

2.1. As noted in the Automation memo, solely automated decision making is the ability to make decisions by technological means without human involvement[7]. Three issues are relevant here:

2.1.1. Decision: according to literature[8], "decision" is viewed in a generic sense and indicates a particular attitude or stance taken towards a person that has a degree of binding effect, in the sense that it must – or at the very least, is likely to be– acted upon. In the SSAD context, the decision will be the recommendation that personal data should be released and/or the eventual decision as to whether or not personal data of a registrant should be disclosed to third parties.

2.1.2. Data processing (i.e. what data needs to be processed for the decision, and more specifically, whether it is necessary for the registrant's personal data to be processed as part of the decision): In one of the scenarios considered above, you mention that "*the Central* Gateway *makes a decision without processing the personal data*". We understand this means that the Central Gateway will not have access to and will not consider the requested non-public data in the decision making. We have considered if this would mean that Art.22 is not applicable.

2.1.3. First, the EPDP team should note that, the processing which is covered by Art. 22 GDPR can be wider than the processing of the affected individual's personal data and does not require the decision to be made only on processing of the affected individual's (registrant's) personal data. In this regard, WP251 provides the example of a credit card company which takes decisions to reduce a customer's card limit based on the analysis, not of that customer's repayment history, but of the behaviour of other individuals who live in the same area and shop at the same stores as the customer. In this case, the personal data of third parties are used in the decision making process. However, in order for the GDPR to apply, there must be some processing of personal data, wholly or partly by automated means, or processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system . So, in the example above, the credit card company does process personal data when it determines that the credit history of geographically close customers is significant for the cardholder.

2.1.4. The definition of personal data is very broad and covers *any* information relating to an identified or identifiable individual[9]. Identifiable individual is one who can be identified either directly or indirectly, in particular by reference to an identifier (such as name, ID number, location data, online

[7] Definition provided in WP251 Guidelines, p. 8.
[8] "*The EU General Data Protection Regulation (GDPR)*", Edited by Christopher Kuner, Lee A. Bygrave, Christopher Docksey, and Assistant Editor Laura Drechsler. Article 22 commentary, p. 532.
[9] Art. 4(1) GDPR.

identifier, etc.). Recital 26 GDPR suggests that "to determine whether a natural person is identifiable, account should be taken of all the means *reasonably likely* to be used, such as singling out, *either by the controller or by another person* to identify the natural person directly or indirectly" (emphasis added). Recital 26 further explains that to ascertain whether means are reasonably likely to be used to identify the individual, "*account should be taken of all objective factors*, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments" (emphasis added).

2.1.5. CJEU case law pre-dating GDPR also takes this approach: in the "Breyer case" (Case C-582/14), the Court ruled that dynamic IP addresses collected by an online media services provider may still constitute personal data because it was reasonably likely that other parties would be able to identify the owner of the IP address. For example, the Court found that in the event of cyber attacks the online media services provider would be able to contact the competent authority, so that the latter could take the steps necessary to obtain that information from the internet service provider and to bring criminal proceedings.

2.1.6. On this basis, we consider it likely that the decision making *will* involve the processing of personal data, as the request will in most cases be made in respect of a specific domain name assigned to a registrant, where the objective of the request is to obtain more information about the registrant. Besides, the reasons given to support the request for disclosure (for example, crime investigation, trademark infringement) would also relate to the registrant (as well as to the Requestor) and would be personal data relating to the registrant.

2.1.7. As a result, we consider that Art.22 GDPR can apply even if the Central Gateway does not have access to the requested registrant data that forms the subject of the decision. We note however that not obtaining registrant data in advance of the decision might help with complying with other GDPR provisions, for example, the data minimization principle.

2.1.8. From the use cases presented to us, only two seem to not involve the processing of personal data at all, namely: (i) the request for city field only for statistical purposes assuming that no other personal information is presented, and (ii) the request for registrant records which do not contain personal data. Save for these two use cases, the rest would meet the "data processing" criterion.

2.1.9. Whether the decision is solely automated: this will be the case where there is no meaningful human involvement – that is a meaningful oversight of the decision by someone who has the authority and competence to change the

decision[10]. In Scenario 1.a., where the automation is limited to the recommendation and the Contracted Party can take a decision which deviates from the recommendation, this criterion would not apply. In the rest scenarios, we have assumed there will not be (meaningful) human involvement, hence the decision would be solely automated.

2.2. The below table summarises how the first Art. 22 criterion (decision based solely on automated processing) applies to the scenarios presented to us:

Scenario	Decision	Data Processing	Solely automated processing
1.a. Automated recommendation – subject to CP's review	✓	✓	✗
1.b. Automated decision – no meaningful CP involvement	✓	✓	✓
2.a. Automated decision by Central Gateway based on review of registrant's non-public data	✓	✓	✓
2.b. Automated decision making without review of requested registrant data	✓	✓	✓

3. Legal or similarly significant effects

3.1. The second criterion of Art 22(1) GDPR is that the decision produces legal effects concerning the individual or similarly significantly affects them. The GDPR does not explain either term. WP251 attempts to examine these concepts further:

(a) Legal effects affect a person's legal rights (e.g. freedom to associate with others or take legal action), their legal status or their rights under a contract.

(b) Similarly significant effects have an impact equivalent to legal effects or are similarly significant: WP251 states that the effects must be "*sufficiently great or important to be worthy of attention*". WP251 considers that this would be the case where the decision has the potential to:

(i) Significantly affect the circumstances, behavior or choices of the individuals concerned;

(ii) Have a prolonged or permanent impact on the data subject; or

(iii) At its most extreme, lead to the exclusion of or discrimination towards individuals[11].

WP251 acknowledges that it is difficult to be precise about what would be considered sufficiently significant; nevertheless, it seems to set an elevated threshold[12].

[10] Guidelines WP251, p. 21 "*The controller cannot avoid the Article 22 provisions by fabricating human involvement*". This is further examined in the Automation memo (para 1.15), where we note that human involvement as a token gesture will not alter the solely automated character of the decision-making.
[11] WP251, p. 21. For further analysis on this point, see Automation memo, paras 1.10 – 1.11.
[12] Automated decision making had traditionally been subject to diverging approaches across EU Member States under the Data Protection Directive. We have checked supervisory authority guidance in the UK, France,

3.2. Proximate cause: Based on the literature searches we have carried out, there is no case law addressing this and little guidance on the role of proximate cause in determining the legal or similarly significant effects of a decision. There is some discussion of this in German literature, where the majority view is that a decision does not have a "legal effect" where it serves the *preparation* of a legal effect, but does not by itself determine such effect, which occurs at a later stage and by means of a separate action. For example, filing for a default summons does not trigger a legal effect because the legal effect is at a later stage determined by the court – and therefore not by the applicant[13]. The above discussion and example are provided only in the context of examining legal effect and not "similarly significant" effects. We think the same distinction, between preparatory steps and the actual effective decision, could be maintained and that the argument is still helpful here. However, given the broader wording of the "similarly significant" effects criterion, the point is not clear. Given the lack of wider discussion on this point, this is a topic where the views of supervisory authorities could be useful.[14]

3.3. Decision to disclose personal information to a third party: As noted in the Automation memo (para 1.9), the decision to disclose personal data via the SSAD would not in itself produce a legal effect on a registrant: this would depend on the action of the requestor. However, unless the notion of proximate cause is accepted, it is possible that the decision to release could be "similarly significant". We understand that one purpose of the use cases is to provide clarity as to types of disclosures where disclosure would not pass this threshold, Analysis of each use case is set out under para 3.4 below.

3.4. Assessing effect of disclosure under each use case: In order to assess whether a use case produces similarly significant effects, the purpose of disclosure must be clearly defined – this was not the case in some of the use cases presented and we have indicated where this is relevant. Refining these further would facilitate singling out cases which are not caught by Art. 22 GDPR. In principle, where the purpose of disclosure is crime detection, prevention and prosecution, the decision would most probably be deemed to have a legal or similarly significant effect. However, disclosure of data for these purposes would also be one of the cases (probably the most relevant in practice) where a Member State derogation could apply. In such case, the assessment of whether or not the disclosure has a legal/similarly significant effect would not be required and the automation of the decision would be permitted on the grounds of the derogation (see para 4.1 below).

Germany and Belgium and they seem to largely follow WP251 Guidelines; however, the review of guidance in other key jurisdictions might be useful, in order to establish a uniform and consistent approach.

[13] BeckOK DatenschutzR/von Lewinski, 31. Ed. 1.2.2020, DS-GVO Art. 22 Rn. 32; Simitis/Hornung/Spiecker gen. Döhmann/P. Scholz, Datenschutzrecht, DSGVO Art. 22 Rn. 34

[14] The EPDP Team has also asked under question C.4 what the risk of liability would be to 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. The essence of the question is whether a decision to release data to a Requestor, where it is known that the Requestor will use the data in a way that will have legal or similarly significant effect for the individual, could itself be regarded as a decision with similarly significant effects. The comments above about proximate cause, and the distinction between preparation and final decision are pertinent. We think that the situation would be different if the Central Gateway /CPs have no reason to believe that the data will be used in this way, although, in the time available, we have not researched this point.

3.4.1. LEA in same jurisdiction as CP or competent data protection authority investigating a criminal offence under data protection legislation: We understand that disclosure in this case would be made for the purposes of crime investigation, detection, prevention and prosecution: use of data for such purposes could often have a legal or at least similarly significant effect on registrants. One of the proposed safeguards is to require recipients to confirm that data will not be used in a manner that has legal effects on the registrant; it would be useful to understand more about how realistic this safeguard would be for a Requestor with this use case.

3.4.2. Competent data protection authority investigating a complaint: we examined this use case separately, because data protection ("supervisory") authorities which are independent authorities would usually carry out administrative processes. We have identified two possible purposes here:

(a) The investigation of an infringement of data protection legislation allegedly committed by the registrant; or
(b) The investigation of an infringement of the data protection legislation allegedly committed by ICANN/CPs affecting the registrant.

In the first case, the investigation of a violation of law could be considered to significantly affect the circumstances of the individual and thus have a similarly significant effect. In the second case, the disclosure of data would not be likely to have a significant effect on the registrant.

3.4.3. Request for City field only:

- to evaluate whether to pursue a claim : based on previous discussions, we understand that the City field may in some instances be required in order to assess whether or not the jurisdiction to which the registrant is subject would be favourable to the exercise of the type of legal claim in which the Requestor is interested. Such purpose does not seem to significantly affect the registrant: the decision for disclosure does not seem to have the potential itself to affect the legal rights or the legal status of the registrant or to significantly affect their circumstances. Also, it would not itself result in a legal claim; besides, in most cases the disclosure of this information alone would not allow the identification of the registrant.
- for statistical research purposes: it seems unlikely to us that this purpose would amount to a legal/similarly significant effect.
- for other non-legal purpose: it is unclear what those purposes would cover. We suggest clarifying the purpose of the disclosure in a more specific manner.

Given the conclusions in the *Breyer* case (under para 2.1.5. above), it may be difficult to demonstrate that release of City field in connection with potential litigation will not still amount to processing of personal data. However, this would not necessarily alter the above assessment under the first bullet point (as the decision to disclose the data given these safeguards would not have a legal (or similarly significant) effect).

3.4.4. Registration record contains no personal data and has already been disclosed: where the decision does not relate to an individual and does not involve personal data, the assessment of legal/similarly significant effects is not relevant. In this case, there is also no need for the restriction that this data has already been disclosed. We understand that this may be the reason the parties are confident that there is no personal data involved, but there could also be other ways of addressing this.

3.4.5. Registration record has already been disclosed under the same authorization assertions to a requestor of the same type: this would depend on the purpose of the original and the envisaged disclosure. The fact that the data has already been disclosed under similar circumstances does not preclude the likelihood of the new disclosure having a significant effect on the registrant.

3.4.6. "Clear cut" TM claim:
-to contact the registrant: this would depend on the purpose of contact. Further clarity would be helpful.
-to file a claim: the disclosure of data for the purpose of exercising a trademark claim against the registrant would most probably significantly affect the circumstances of a registrant.

3.4.7. Request for data from ICANN compliance: it is unclear for which purpose the disclosure would be made here – we suggest clarifying this point further. For example, if the disclosure is made for audit purposes, it is likely that the decision would not have legal or similarly significant effects.

3.4.8. Identify infrastructure involved in botnets, malware, phishing, and consumer fraud:
-to investigate infrastructure: where there is no expectation that legal action can or will be taken, then the mere investigation by a cybersecurity professional might not indicate legal or similarly significant effect.
-to share with LEA to take legal action: this purpose would likely constitute a legal or similarly significant effect (for the same reasons as the use case under 3.4.1. would do so).

3.4.9. Request for data from a UDRP/USR Provider to respond to verification request required under the Policy: from Art. 4(b) of the Rules, we understand that the verification request is made for the purpose of validating the data of the Complainant and ensuring it is accurate. If this is the case, we do not consider this verification to constitute a legal or similarly significant effect. In any event, it would be helpful to specify the purpose of the disclosure further.

3.5. Summary table

Use case	Purpose	Legal/ similarly significant effect		
		🔴 Yes	🟡 Unclear	🟢 No
LEA/ DP authority in same jurisdiction as CP	Crime prevention/detection/prosecution	🔴		
DP authority	Investigation of data protection infringement allegedly committed by registrant	🔴		
	Investigation of data protection infringement allegedly affecting registrant	🟢		
Request for City field only	Evaluate whether to pursue a claim	🟢		
	Statistical purposes	🟢		
	Other non-legal purposes	🟡		
No personal data on registration record previously disclosed	If there is no personal data and the decision does not relate to an individual, this assessment is not relevant	🟢		
Registration data already disclosed to same type Requestor under same authorisation assertions	Currently unclear purpose – the assessment depends on the purpose of the initial and the current request	🟡		
"Clear cut" trademark claim	Contact registrant	🟡		
	Exercise trademark claim	🔴		
Request from ICANN compliance	Not specified purpose (further clarification required)	🟡		
Request to identify infrastructure involved in botnets, malware, phishing and consumer fraud	Mere investigation	🟡		
	Share data with LAE and take legal action	🔴		
Request for data from a UDRP/USR Provider.	Mere investigation	🟡		

4. Alternatives to Art. 22 GDPR

4.1. EU or Member State derogations as alternative to Art. 22 processing: As discussed under para 1.6 above, EU or Member State law may impose restrictions to the application of Art. 22 GDPR, among other provisions, in certain situations. It is possible that some Member States may have introduced restrictions which could be applicable to the SSAD: in such cases, ICANN could automated the decision making process without carrying out the analysis under Art. 22 set out above. Of course, as noted above, this would require further analysis on a Member State specific level and would add to the complexity of the SSAD.

4.2. By way of example, Ireland's Data Protection Act 2018 includes a provision at s. 60(3)(ii)) to the effect that data subject rights (including Art.22) "are restricted" to the extent that the restrictions are necessary and proportionate for, inter alia, the prevention, detection, investigation and prosecution of criminal offences. On the other hand, restrictions established in the UK, Belgium and Germany would not be relevant/ applicable to the SSAD.

4.3. Alternative to Art. 22 GDPR examined in Automation memo: In para 1.12 of the Automation memo, we suggested that an alternative measure of self-certification would possibly fall outside the scope of Art. 22. This was based on the argument that this measure would not amount to a decision. According to the Shorter Oxford English Dictionary, "decision" is defined as:

- "*the action of deciding a contest, dispute, etc.; settlement, a final (formal) judgement or verdict;*
- *"the action of coming to a determination or resolution with regard to any point or course of action a resolution or conclusion arrived*".

4.4. Accordingly, an action that does not include a resolution or an act of determination would not meet the above definition. The situation where a Requestor receives the requested data by merely ticking all the boxes, would arguably not constitute a decision that would be caught by Art. 22 GDPR. However, as noted in para 1.13 of the Automation memo, the parties controlling the SSAD have an obligation to take appropriate measures for the security of the data they hold, in particular to implement measures to prevent an unauthorised disclosure of data to third parties – in this context, a self-certification mechanism would likely not be deemed an appropriate security measure to safeguard the integrity and confidentiality of personal data.

5. Additional safeguards and transparency considerations

5.1. Safeguards: At a general level, the safeguards set out in Appendix 1 are helpful. In addition to these, we have outlined in Appendix 2 of this memorandum additional safeguards that ICANN could consider implementing – irrespective of whether or not there is automated decision making in the sense of Art. 22 GDPR. Given the variety of requests, the different use cases presented and the different legal requirements that may apply in each relevant jurisdiction, we have examined additional safeguards at a higher level that would be relevant for the majority of use cases. The list of safeguards and measures suggested in Appendix 2 is not exhaustive and further measures may be required or appropriate depending on the relevant jurisdiction and the circumstances of the request.

5.2. Transparency considerations

5.2.1. Complying with Art. 13 – manner of providing information: the existence of an automated decision (whether or not that decision falls under Art. 22 GDPR) does not alter the manner in which information is to be provided. The relevant information will typically be included in the controller(s)'

privacy notice which must be provided to the registrant at the point of the collection of their data.

5.2.2. The general transparency requirements will also apply here: the information must be provided in a concise, transparent, intelligible and easily accessible form, in a clear and plain language[15]. This means:

- Efficient and succinct communications to avoid information fatigue;
- Privacy notice clearly differentiated from non-privacy related information, such as contractual terms;
- Where appropriate, use of layered privacy notice and just-in-time notices;
- Spell out the most important consequences of the envisaged processing[16].

5.2.3. The disclosure of registrant data in response to legitimate third party requests is an important element of the Domain Name system. As these disclosures could have a considerable impact on individuals on some occasions, it would be appropriate to bring this activity and its consequences to the attention of individuals, either by making the relevant reference in the privacy notice more prominent (e.g. using bold text or put in prominent position), or also in the form of a short notice at the point of collection of registrant data.

5.2.4. Who will provide the information: the obligation to provide information rests with the controller:

- In the case of joint controllers, the parties can arrange between them how they will comply with their transparency requirements in respect of the joint processing activity[17]. In such case, it would seem appropriate that registrars make this information available to registrants, as they have a direct relationship with registrants.
- In a scenario where CPs are not controllers in respect of the SSAD (see relevant para 6.1.9 below), it may still be appropriate for registrars to provide this information to registrants (considering that registrars have a direct relationship with them). However, in this situation, the notice should make clear to registrants that registrars do not act as controllers in respect of the SSAD; this could be achieved by providing a separate statement specific to the SSAD which would identify the applicable controller(s).

5.2.5. Timing: Information must be provided at the point of collection of registrant data[18]. The GDPR states that when the data has not been obtained directly from the individual, information shall be provided at the latest within one month after obtaining the data – or, if disclosure to

[15] Art. 12(1) GDPR.
[16] Article 29 Working Party Guidelines on transparency under Regulation 2016/679, WP260 ("*WP29 Transparency Guidelines*"), approved and adopted by the EDPB.
[17] As per Art. 26(1) GDPR, the joint controllers shall determine their respective duties to provide the information referred to in Arts. 13 & 14 GDPR.
[18] Art 13(1) GDPR.

another recipient is envisaged, at the latest when the personal data are first disclosed[19]. This provision would be relevant in scenario 2, where ICANN and/ or the Central Gateway (rather than the CPs) will be considered controllers in respect of data processing in the SSAD. Given the circumstances of processing in the SSAD (in particular, the often confidential nature of the disclosure of data), we consider that an appropriate way to provide this information would be for the CPs to be required to provide a privacy notice along with their own privacy notice at the point of collection of registrants' data: for example, by providing information in the CP's privacy notice and by providing to registrants a link to the relevant controller(s)' privacy notice – in such case, again, it should be made clear that CPs are not controllers in respect of the SSAD.

5.2.6. Content: Art. 13 GDPR sets out a list of points of information about data processing that controllers are required to provide to individuals. The following will be of particular relevance:

- Recipients or categories of recipient of the personal data[20]: The WP29 Transparency Guidelines suggest the default position should be to provide information on the actual (named) recipients and if this is not the case, the controller(s) shall be able to demonstrate why it is fair to take this approach. It seems to us that it would be impossible to name third party recipients in the SSAD context; in some situations, this could also undermine the SSAD's purpose. However, the notice should include an appropriate level of detail - mere reference to "*third parties which submit legitimate requests*" would not be sufficiently transparent. WP29 Guidelines suggest that the categories of recipient should be as specific as possible by indicating the type of recipient (by referencing the activities it carries out, the industry, sector and sub-sector and their location).

- Data transfers[21]: The privacy notice must contain information on transfers of personal data to third countries outside the EEA and the mechanisms used to legitimise these transfers. The WP29 Transparency Guidelines suggest that the notice should explicitly mention all third countries to which the data will be transferred – we appreciate this will be difficult in practice. In terms of transfer mechanisms, please see comments under Liability memo, para 3.17[22].

[19] Art. 14(3)(a) and (c) respectively.
[20] Art. 13(1)(e) GDPR.
[21] Art. 13(1)(f) GDPR states that data subjects should be provided with the following information: "*where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.*"
[22] Para 3.17, where we comment on the use of Standard Contractual Clauses.

- Joint control: If CPs and ICANN are considered joint controllers, the privacy notice should include information about their joint control arrangement, setting out the role of each party, including a contact point for individuals[23]. On the assessment of the role of CPs as joint controllers, see section 6 below.

5.2.7. Content specific to Art. 22: In addition to the above, if the automated decision falls under the scope of Art. 22 GDPR, then controllers have to:

- tell registrants if they are engaging in such automated decision making;
- provide meaningful information about the logic involved: WP29 Art. 22 Guidelines do not require a complex explanation or provision of technical details – they advise that the information provided should be "*sufficiently comprehensive for the data subject to understand the reasons for the decision*". In the SSAD context, this would include providing an explanation of the use cases which will be automated; and
- explain the significance and the envisaged consequences of such processing: WP29 Art. 22 Guidelines suggest that information must be provided about "*intended or future processing, and how the automated decision-making might affect the data subject*" and that "*real, tangible examples of the type of possible effects should be given*". In the SSAD context, this would include explaining the consequences of disclosure of data for each use case which is automated and which has legal or similarly significant effect. As per para 4.4.1.2 above, the most important consequences of the disclosure should be mentioned, irrespective of the application of Art. 22 GDPR.

5.2.8. Impact of Art. 22 processing on the manner of providing information: The manner in which information must be provided is not affected by the application of Art. 22 GDPR. The same considerations (including those set out in paras 5.2.1 – 5.2.5 above) should be taken into account in both scenarios.

5.2.9. The existence of Art. 22 automated decision making will impact though on the *content* of the information to be provided to registrants:

- Greater transparency and the elements set out in para 5.2.7 above will not be required for all use cases: they would be only required where there is Art. 22 processing. Therefore, this additional information will not be relevant to:
  a. Scenario 1.a where the decision making process is not fully automated (only automated recommendation);
  b. Any automated decision which does not produce legal or similarly significant effects; and

[23] Art. 26GDPR requires that joint controllers determine their respective responsibilities by means of an arrangement – the essence of the arrangement should be made available to data subjects.

c. Cases where an exemption to Art. 22 applies under EU or Member State law.

- As indicated under para 1.5 above, of the remaining use cases which meet Art. 22(1) criteria, only those which are authorised by EU or Member State law are permissible (under Art.22(2)). For the rest, an alternative approach must be found (i.e. meaningful human intervention).

- The additional information in para 5.2.7 would be required only for those permissible use cases. In such cases, it is likely that the relevant Member State law requires specific drafting to capture the specifics of any such situations.

- If the relevant Member State law requires disclosure of the data, it would likely be best if the relevant CP is (sole) controller for this disclosure, so as to avoid the complexity of Central Gateway making the disclosure but not being subject to the relevant law requiring the disclosure. In such case, information pertaining to the specific use case of the required disclosure will need to be included in CP's privacy notice.

5.2.10. Interaction between the right to information and the right of access: The right to information (Arts. 13 & 14 GDPR) and the right of access (Art. 15 GDPR) are two distinct rights: the first takes the form of an obligation on controllers to provide individuals with information about the processing without individuals having to exercise this "right" ("notification duty" – this is in principle satisfied by means of providing a privacy notice), while the right of access has to be specifically invoked by individuals. The provision of information under Arts. 13 & 14 GDPR does not affect the right of registrants to request access to their personal data. This means that an access request cannot be refused on the basis that the same information has been provided in the privacy notice. However, Art. 15 GDPR requires the provision of a set of information which is nearly identical to the information that needs to be provided under Arts. 13 & 14 GDPR. This means that some of the information to be provided under the right of access might be the same as the information already provided in the privacy notice. The following difference in the wording used by Art. 15 GDPR is particularly relevant to the SSAD: whilst Arts. 13 & 14 refer to information about "the recipients or categories of recipients of the personal data"[24], Art. 15 refers to "the recipients or categories of recipient to whom the personal data *have been* or will be disclosed, in particular recipients in third countries or international organisations" (italics added)[25]. This indicates that if at the time the registrant submits an access request, their data has been already disclosed to a third party, the registrant should be in principle entitled to this information – unless an exemption applies.

[24] Arts. 13(1)(e) and 14(1)(e) GDPR respectively.
[25] Art. 15(1)(c) GDPR.

Recital 63 GDPR contends to this view: it states that individuals should have the right of access to their personal data "*in order to be aware of, and verify, the lawfulness of the processing*". Informing registrants of the parties who have accessed their personal data (either by name or by category) may assist them in verifying that such disclosure has been lawful.

5.3. However, disclosing this information may not always be required. The right of access is not an absolute right – Art. 23 GDPR allows EU or Member State law to introduce restrictions to the right of access in certain circumstances, for example, where it is necessary for the prevention, detection, investigation and prosecution of criminal offences[26]. For example, the UK Data Protection Act 2018 establishes an exemption from the right of access (both from the provision of a copy of personal data and the information relating to processing) for the prevention or detection of crime, or the apprehension or prosecution of offenders, to the extent that the fulfilment of such right would be likely to prejudice these purposes[27].

5.4. Right to explanation: It has been debated in literature whether or not the GDPR establishes the right to explanation of automated decisions that fall under Art. 22 GDPR, i.e. the right of individuals to obtain information about the logic and the individual circumstances of a specific decision, after such decision has been made[28]. Considering the circumstances of the SSAD, we note that such debate would not be of particular relevance to the decisions taken in the context of the SSAD, for the following reasons:

(a) The cases where the parties will be allowed to use Art. 22 automated decision making will be limited – effectively this will be allowed when authorised by EU or Member State law which should already lay down suitable measures to safeguard individuals' rights and freedoms and legitimate interests (per Art. 22(2)(b) GDPR);

(b) Individuals will effectively obtain the same information by exercising their right of access in combination with their right to information. Under the right of access, individuals must be informed of the recipients who have received their personal data (unless an exemption applies): this will inform registrants of whether a disclosure has been made. In addition, we understand that the logic behind the automated decision making will always consist of a set of objective, pre-defined rules for each use case and will not be affected by factors relating to the registrant's circumstances: this means that the information owed under an *ex post* right to explanation would essentially be the same as the *ex ante* information provided to registrants as part of Arts. 13 & 14 requirements and the information to be provided under

[26] Art. 15 GDPR also introduces a restriction to the access right, by stating that the right to obtain a copy of the personal data undergoing processing "*shall not adversely affect the rights and freedoms of others*" (Art. 15(4) GDPR). However, this restriction might not be particularly helpful here, as it seems to apply only to the copy of the personal data requested (Art. 15(3) GDPR) and not the set of information relating to the processing, which includes the recipients (Art. 15(1) GDPR).

[27] UK Data Protection Act 2018, Schedule 2, Part 1, para 2.

[28] For example: Wachter et al, "*Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*", 2017, which argues that the GDPR does not provide for a legal basis for a right to explanation of specific decisions and Bryce Goodman and Seth Flaxman, "*EU Regulations on Algorithmic Decision-Making and a "Right to Explanation""*, 2016, which takes the opposite view.

Art. 15(1)(h) GDPR; hence the analysis of whether the GDPR establishes an ex post right to explanation would become superfluous in the SSAD context.

Therefore, we consider that the existence of a right to explanation would not substantially alter the controller(s)' transparency obligations.

6. Status of parties and liability

6.1. Status of the CPs as (independent/joint) controllers / processors: In the Liability memo, we examined the status of CPs as controllers or processors. We concluded that CPs would more likely be joint controllers with ICANN org in respect of the SSAD, rather than processors. This was based on the premise that CPs typically act as and are viewed by registrants as controllers (*presumption of control*), disclosure of data to Requestors is associated with the role of CPs and is likely to be seen as an inevitable consequence of being a CP (*difficulty presenting CPs as acting "on behalf of" someone else*), and that EU case law establishes a low threshold to become controller both in respect of determining the purpose and the means of processing.
We have previously commented that supervisory authorities will likely start from an assumption of joint control and this was also pointed out by the Belgian supervisory authority in its recent letter to ICANN[29]. We have also noted that the EDPB is working on a new Opinion on the controller/processor status; however, this has still not been issued.

6.1.1. Scenario 1 (1.a.& 1.b): Under scenario 1.a, the Central Gateway would receive requests from accredited users and would make an automated recommendation of disclosure, while the **ultimate decision to disclose would continue to rest with the CPs**. The analysis carried out in the Liability memo would continue to apply. There does not seem to be a factual change in the role of CPs that would trigger a further analysis or that could justify deviating from our initial conclusions.

6.1.2. Under Scenario 1.b., CPs with "*enough confidence*" in the Central Gateway and its recommendations, may choose to automate the decision to disclose data to third parties. Under this scenario, the control of the CPs over the *purpose* of processing would not be altered – the same considerations as those set out in the Liability memo continue to apply. In respect of the *means* of processing, CPs would entrust the Central Gateway to carry out the decision-making process; however, CPs would continue to "own" the ultimate decision to disclose data and ultimately would have control over the means of processing, since they would control whether or not the decision will be fully automated and they would have the power to alter the means of processing (e.g. move to a model including human intervention). As a result, we consider that our previous analysis as to the status of CPs would continue to apply in Scenario 1.

6.1.3. Scenario 2 (2.a & 2.b): The second scenario provides that the decision to disclose the registrant data would be taken by the Central Gateway without the relevant CP being able to review the request. The CPs would have a

[29] Letter of the Belgian Data Protection Authority to Göran Marby, dated 04/12/2019.

contractual obligation to provide data to the Central Gateway – either before or after the decision of disclosure is taken by the Central Gateway.

6.1.4. As previously noted, the status of a party as controller or processor is not a matter of contractual designation – it is a matter of legal designation, implied competence (presumption of control) or factual assessment[30]. This was also pointed out in the Belgian DPA's letter[31]. Therefore, where there are elements that point to the CPs being considered controllers, this would not necessarily be altered by contractual provisions that require CPs to disclose the data to the Central Gateway.

6.1.5. Macro-level approach under EU guidance: Opinion WP169[32] suggests that on occasions it would be appropriate to adopt a macro-level approach when examining whether a party has joint controller status[33]. Under this approach, (i) the transfer of data from CPs to the Central Gateway (operated by or on behalf of ICANN) for the purpose of the Gateway evaluating and processing requests for disclosure and (ii) the subsequent disclosure of that data by the Central Gateway to the Requestors would likely be considered as a "set of operations" pursuing a joint purpose. In this context, the purpose and means of processing would probably be considered "*closely linked*[34]" in such manner that the CPs and ICANN would be considered as joint controllers. In this context, it is likely that the contractual arrangement between ICANN and CPs would be seen by supervisory authorities as an allocation of tasks between controllers, rather than purely as an act of processing pursuant to the instructions of, and on behalf of, ICANN org.

6.1.6. Although ICANN org will have an elevated level of control in the context of the SSAD, this does not in itself preclude CPs' control: according to Opinion WP169, "in the context of joint control the participation of the parties to the joint determination may take different forms and does not need to be equally shared. Indeed, in case of plurality of actors, they may have a very close relationship (sharing, for example, all purposes and means of a processing) or a more loose relationship (for example, sharing only purposes or means, or a part thereof)" (emphasis in original).

6.1.7. The use of the macro-level approach and the above considerations indicate that CPs would be likely to be considered joint controllers with ICANN in the context of the SSAD.

6.1.8. Micro-level approach of EU case law: Opinion WP169 dates from 2010; more recent cases from the CJEU – in particular the *Fashion ID* case – have

[30] WP29 Opinion 1/10 on the concepts of "controller" and "processor" ("WP 169"),available here.
[31] Letter of the Belgian Data Protection Authority to Göran Marby, dated 04/12/2019.
[32] WP29 Opinion 1/10 on the concepts of "controller" and "processor" ("WP 169"), p.22.
33 Ibid, p. 22, "*In some cases, various actors process the same personal data in a sequence. In these cases, it is likely that at micro-level the different processing operations of the chain appear as disconnected, as each of them may have a different purpose. However, it is necessary to double check whether at macro-level these processing operations should not be considered as a "set of operations" pursuing a joint purpose or using jointly defined means*".
[34] Ibid, p. 20, Example No. 10.

supported a closer, analysis focusing on specifically defined elements of processing[35]. These cases suggest that there is a low threshold to become a controller; the test, according to the CJEU, is whether one "*exerts influence over the processing of personal data, for his own purposes, and (…) participates, as a result, in the determination of the purposes and means of that processing*"[36]. The Fashion ID case further suggests that a party may be a controller jointly with others "*only in respect of operations involving the processing of personal data for which it determines jointly the purposes and means*". The Court further ruled that by contrast, a party cannot be considered controller in the context of operations that precede or are subsequent in the overall chain of processing for which that party does not determine either the purposes or the means. The Court considered that Fashion ID was a controller just for the collection of data via a Facebook like button embedded on its website; the Court assumed that it would be impossible for Fashion ID to be a controller for processing of the data after its transmission to Facebook, on the basis that it was impossible for it to determine the purposes and means of the subsequent operations carried out by Facebook[37]. Far from taking a "macro" approach to the analysis, the Court looked at processing at a detailed, micro, level.

6.1.9. The divergent approaches followed by the Opinion WP169 and the CJEU demonstrate the lack of clarity in this area and the difficulty of reaching safe conclusions in respect of the status of an entity, especially pending the publication of the EDPB Opinion on controllers and processors. In the light of the *Fashion ID* case, we think there is a good argument that in Scenario 2 the CPs would *not* have sufficient control over the decision making process and the disclosure of data to Requestors and so would not be joint controllers in respect of these activities. However, the fact that CPs are not controllers in respect of the disclosure of data to Requestors would not affect their responsibility – as controllers - for disclosure of data to the Central Gateway. As explained above and in the Liability memo, it would not be plausible to argue that CPs are processors for disclosure of data to Central Gateway merely by virtue of a contractual commitment to make the disclosure.

6.1.10. The impact of this on the liability of CPs is further examined under para 6.2 below.

6.1.11. Outsourcing the decision making to an independent professional[38] service provider: We have been asked to give our view on the role of ICANN and CPs in the scenario where the Central Gateway outsources the decision making to an independent legal/professional service provider. We do not consider that outsourcing the decision making would have an impact on the relationship

[35] CJEU judgement in case C-40/17 Fashion Id, at [74].
[36] Ibid, at [68], C-210/16 at [38].
[37] Ibid at [76].
38 We note that the instructions refer to a "*legal* service provider": because of the specific regime and regulatory framework of the provision of legal services, and assuming that the outsourcing of the decision making in this context would not be the subject of reserved legal services, we have considered a broader category of professional service providers to allow for more flexibility in our assessment.

between ICANN and the CPs; it does not alter any of the factors relevant to determining if the CPs would be a joint controller. However, this outsourcing could *possibly* mean that the independent provider would act as controller (depending on whether the provider has sufficient power and autonomy in decision making). On a relevant point, we also note in Exhibit 1 the presumption that the Central Gateway would act as controller of registrant data (only) where it requires the data for the decision making process. The EPDP team should note that the assessment of whether or not the Central Gateway acts as controller or processor of registrant data would not depend on whether it obtains physical access to such data before or after the decision making. It rather depends on the level of autonomy it has over the decision making process and the disclosure of data to third parties.

6.2. Risk of liability: When examining the risk of liability of CPs, two factors are relevant, both of which are considered in detail in the Liability memo:

6.2.1. The status of CPs as controllers, joint controllers, or processors (which we examined above and where we suggest that the possibility of CPs being processors can be dismissed). In this respect, we would stress the importance of allocating tasks and responsibilities between joint controllers, as per Art. 26 GDPR. A clear allocation will allow certainty over the elements of compliance each party is to undertake and subsequently each party's level of responsibility; and

6.2.2. The type of liability, i.e. civil liability and liability to enforcement action (e.g. administrative fines) by supervisory authorities. In brief:

(a) Liability towards individuals (i.e. compensation for damage resulting from an infringement of the GDPR): Where there are joint controllers, Art. 26 provides that a data subject may exercise rights against any of the joint controllers on a joint and several basis. However, under Art. 82, controllers, joint controllers and processors who are involved in the "same" processing are also subject to joint and several liability. This means that CPs can be held liable for the entire damage caused by processing they are involved in, irrespective of their status as joint controllers or separate controllers. The GDPR sets out a statutory right to recover an appropriate amount of the compensation that was paid out (Art. 82(5) GDPR). Parties are excluded from this liability if they prove that they are not in any way responsible for the effect giving rise to the damage (Art. 82(3) GDPR). On this basis, we think that Scenario 2 offers least risk of liability to CPs. If CPs are not joint controllers, then there is no automatic joint and several liability under Art.26. As CPs have less involvement in disclosures under Scenario 2, it may also be easier for them to demonstrate that they are not involved in the "same" processing and so are not jointly liable under Art.82. If, notwithstanding this, they were held to be involved in the "same" processing, then they would have stronger arguments (by comparison to Scenario 1), to show either: 1) that they were not "in any way responsible for the event giving rise to the

damage" – so as to claim exemption from liability under Art.82(3); or 2) to claim back any compensation paid, on the basis that ICANN org, or the Central Gateway, is actually responsible for the damage.

(b) Liability to supervisory authorities (i.e. enforcement action, such as monetary penalties): it is less clear that a strict joint and several liability regime would apply here for joint controllers. On the contrary, there is scope to argue that enforcement action should be imposed based on the "degree of responsibility" of the party. Again, however, this means that Scenario 2 poses least risk of liability for CPs, as – under this scenario – they have no responsibility for disclosure of data to Requestors (if they are not controllers at all for this) and they would also have less responsibility for this if, contrary to the points above, they were held to be joint controllers.

Appendix 1 – Safeguards and use cases

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

Assumptions:

I. All requestors have been accredited by Accreditation Authority and all requestors are individually authenticated by the Gateway.

II. All requests are syntactically correct and complete, including any/all required Authorization Assertions.

III. 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.

IV. 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.

V. 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.

VI. CPs shall provide feedback about the quality of past recommendations to the Gateway in order to improve the recommendation of future recommendations.

VII. 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.

VIII. As more legal certainty is acquired, additional use cases may be added to this list.

IX. 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**

    a. Examples

        i. Law Enforcement Agency from Jurisdiction A requests Registrant RDS data from a Registrar also in Jurisdiction A

        ii. Competent DPA requests data in response to a Data Subject complaint that their data is being misused in violation of the GDPR

b. For the Gateway to make a good recommendation, access to the City field may be required; see below

2. **Request for City Field (only)**

   a. Examples

      i. Requestor submits a request for the City field in order to ascertain which specific jurisdiction to make a legal claim, or

      ii. Requestor submits a request for the City field for the purpose of statistical research or similar non-legal purpose

   b. 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.

      i. 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**

   a. 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.

      i. The flag remains valid so long as none of the data fields have changed.

   b. The Gateway shall determine whether any data fields have changed by inspecting the Public RDS/WHOIS data.

   c. The flag could be stored at either the CP and/or in the Gateway.

   d. A registrar could optionally implement a system to flag such a domain for automation when the data is collected, to enable later automation.

   e. NOTE: Some TLDs are not expected to contain any personal data, and this can streamline processing.

      i. See .BANK, .INSURE, .MUSEUM, and others

      ii. There may be other TLDs whose registries enforce policies requiring disclosure, even for personal data, which may streamline processing

      iii. 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**

   a. Once registration data has been disclosed, it can be flagged for automatic disclosure in future requests if

i. The same authorization assertions are used, and

ii. The requestor is of an equivalent type to the previous one, and

iii. None of the contact data fields have changed

iv. 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

b. Gateway can determine whether any data fields have changed by inspecting the Public RDS/WHOIS data

c. The flag includes details of the previous assertions and previous disclosed-to entity type

d. The flag could be stored at either the CP and/or in the Gateway.

e. A registrar could optionally implement a system to flag such a domain for automation when the data is collected, to enable later automation

f. 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. **<u>"Clear cut" TM claim</u>**

a. 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.

i. The trademark exists in the Trademark Clearinghouse (TMCH)

ii. The trademark must be "live" (not just applied for, rejected or expired)

b. TM owner has proved it has "agency" to request this data

i. The owner of the TM, or

ii. Entity acting on behalf of the owner

c. Limits

i. The trademark string is of sufficient length/complexity that collisions with non-trademark strings is very unlikely (e.g. "microsoft")

ii. 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

iii. Automation would not work for figurative marks or where the domain name is allegedly confusingly similar to the trademark.

iv. 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.

v. 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**

a. 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)

b. ICANN must agree to be a controller for the purpose of this processing.

c. 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**

a. Requestor is accredited as a cybersecurity professional and has agreed to comply with specific cybersecurity codes of conduct, if applicable.

i. Not everyone can simply assert that they are such a professional.

b. Requestor represents that it has investigated and confirmed that the domain name is being used as part of a criminal infrastructure.

i. Direct evidence can also be included in the request - based on the Request contents building block.

c. 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.

a. UDRP or URS Provider has received a UDRP or URS filing for the domain name.

b. 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:

I. All requestors have been accredited by Accreditation Authority and all requestors are individually authenticated by the Gateway.

II. All requests are syntactically correct and complete, including any/all required Authorization Assertions.

III. 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.

IV. 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.

V. 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.

Appendix 2 – Safeguards suggested by Bird & Bird

As per para 5.1 of this memorandum, this Appendix sets out additional safeguards that could be considered in the context of the SSAD.

a. Engage with EDPB/ supervisory authorities: It could be useful to engage with supervisory authorities and seek guidance on topics which are not sufficiently clarified in existing guidance or case law, such as the scope of "similarly significant" effects and the role of proximate cause in assessing these.

b. Authentication of Requestor: As already provided in the existing safeguards, it is important that the identity of the Requestor is verified and that appropriate security measures are implemented to ensure that only genuine Requestors are accredited. We understand this point is being separately addressed by the EPDP.

c. Essential elements of each use case: We recommend that controller(s) clearly identify -as a minimum- the following elements in respect of each (existing and future) use case: the purpose(s) being pursued by the requestor , and, for each such purpose, the data fields to be disclosed, the type of recipient, the applicable jurisdiction, and the effects of disclosure on registrant. We suggest this is set out by purpose, because different purposes might result in different effects on individuals and might require a different lawful basis. If analysis for several purposes is similar, then they could be grouped together.

d. Legal basis: ICANN and -if relevant- the CPs would need to establish a legal basis for the processing (i.e. the data disclosure via the SSAD). We have examined considerations relating to the legal basis and the application of legitimate interests in the Liability memo (para 3.9 et seq.) and the Automation memo. As previously indicated[39], where multiple different controllers are involved, the challenge to establish a legal basis for the processing is greater. The CJEU appears to confirm in recent case law[40] that each joint controller must have a legal basis for the joint processing activity. This seems to rule out arguments that all joint controllers can rely on just one of the controllers establishing a legal basis. In the SSAD context, this could create complexities where only the CP is under a legal obligation to disclose the requested registrant data, while ICANN (or other joint controllers involved in the SSAD) are not subject to the same obligation. For this type of situation, it would be most straight-forward for disclosures to be made as set out in Scenario 1[41].

[39] Liability memo, para 3.9.

[40] See case C-40/17 *Fashion ID,* at [96] the CJEU: *"[…] it is necessary that each of those controllers should pursue a legitimate interest, within the meaning of Article 7(f) of Directive 95/46, through those processing operations in order for those operations to be justified in respect of each of them*".

[41] If it is important for disclosures to be made by the Central Gateway, the alternative would be for the CP to appoint the Central Gateway as a data processor for this specific disclosure. This would, however, undermine the benefits of Scenario 2, set out at Section 6 (Liability) of this memorandum.

e. Terms of disclosure: As the decision on data disclosure depends on information presented by the Requestor, it is important that the Requestor provides sufficient assurances as to the reasons for their request, the envisaged processing and the protection of personal data. The terms should be accepted by the Requestor prior to disclosure of information to them and if the Requestor acts on behalf an organisation (either a private company or a public body), they should provide evidence that they have the authority to bind the organisation and accept the terms on its behalf[42]. We recommend that the terms include the following:

- Purpose limitation: the Requestor must clearly specify the purpose for which it requests access to the data and the consequences to registrants[43] and must undertake not to use the data for other incompatible purposes unless in the following circumstances:
    - For Requestors in the EEA or a country with an adequacy decision: unless permitted by Data Protection law applicable to the Requestor (which will set constraints on this point);
    - For other Requestors: subject to the mandatory requirements of the national legislation applicable to the discloser of the information (i.e. the controller(s) of the SSAD) which do not go beyond what is necessary in a democratic society, if they constitute a necessary measure to safeguard: national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others[44].

  The controller(s) should further consider if there would be situations where they would be interested to control onward disclosure of data more closely.

- Necessity and proportionality: the Requestor shall confirm that the disclosure of data is necessary for them to fulfil the purpose sought, that the requested data is proportionate and that the disclosure of data via the SSAD is the least intrusive way to obtain such data.
- Information to registrant: as explained above, providing information to the registrant that their data has been disclosed to a third party may in some instances be restricted under Member State legislation. As ICANN/CPs may not have all the required information to assess whether an exemption applies to a specific case, it would be helpful if Requestors certified whether providing information to registrants would prejudice the purposes for which registrant data is disclosed to them (for example, may compromise the secrecy of

[42] We note that the rules around authority may differ depending on the jurisdiction and ICANN might be interested to verify requirements in the relevant jurisdictions.
[43] The ICO (UK supervisory authority) notes in respect of law enforcement requests: "Don't be afraid to ask the police why the information is required. You should ensure that personal data is not disclosed unless there is a clear and appropriate justification that takes account of the context for the information request from the police." (communication available here – last accessed 20 April 2020). This indicates the expectation of supervisory authorities that controllers should critically assess requests for disclosure –even if they are made by LAE- and the need to be satisfied that a legal basis applies indeed.
[44] We have followed the approach taken by the 20001 version of the Controller Standard Contractual Clauses on this point.

criminal investigations). The access terms should, however, make clear that the controller(s) would not be bound by this statement and would independently review whether it would be fair to disclose or withhold this information from the registrant.

- Legal/similarly significant effect: the terms could require the Requestor to confirm whether the disclosure would have a legal or similarly significant on individuals (this is also set out in the safeguards under Appendix 1). However, we note that: (a) in some cases this would not be possible (e.g. in disclosures to LAE for the prosecution of criminal offences); and (b) the Requestor's response would not be determinative and the controller(s) of the SSAD would still need to independently consider whether such disclosure would have such effect on the basis of the circumstances of the request.
- Confidentiality: The terms could also stipulate that registrant data is provided to the Requestor on a confidential basis, and that sharing of such data is limited to recipients who have a "need-to-know", provided that appropriate safeguards are in place.
- Data transfers: if the Requestor is based outside the EEA, the terms need to provide for appropriate safeguards for such transfers to be legitimised under the GDPR. In this respect, please see the Liability memo (para 3.17) for our comments on the complications of the use of Standard Contractual Clauses.

f. Security measures: the controller(s) must implement appropriate security measures to protect registrant data, in particular against malicious requests. For example, the SSAD could generate alerts for misuse of the system (e.g. alerts when the same Requestor submits numerous requests for the same registrant data using different use cases).

g. Block bulk requests: disclosure of personal data under bulk requests would be unlikely to comply with the GDPR, hence the controller(s) could implement technical measures to automatically flag and block such requests. See also relevant para 3.11.4 in Liability memo.

h. Legitimate Interest Assessment ("LIA"): Where the disclosure of data relies on the controller(s)' or third parties' legitimate interests, the controller(s) need to carry out a balancing test (otherwise, a LIA) to establish that a legitimate interest applies to the processing and to assess whether the disclosure of data is necessary and proportionate for the pursued interest and is not overridden by the rights and freedoms of individuals. More detailed analysis on this balancing test is included in the Automation memo (paras 2.1 – 2.15).

i. Data Protection Impact Assessment ("DPIA"): the controllers need to consider whether a DPIA is required: for example, this will be the case where the processing is subject to Art. 22 GDPR and is carried out on a large scale (this second criterion would generally apply to the data processed through the SSAD)[45]. Even if not

[45] The WP29 Guidelines on Data Protection Impact Assessment ("DPIA") (available here) provide detailed information on the criteria triggering a DPIA. The two quoted criteria (i.e. large scale processing and automated decision making with legal/similarly significant effects) are the most relevant of the criteria referenced in the Guidelines; however, there may also be criteria at a national level which may be relevant here.

legally mandated, it may still be useful from an accountability perspective to carry out a DPIA.

j. Audits: carrying out regular audits in order to verify the quality of the automated system would be an additional measure to consider. In addition, it would be useful to periodically review the use cases which have been automated to ensure that these remain consistent with legal or regulatory developments.

k. Record of requests: in line with the audit point above, we recommend recording the details of requests, both for internal governance purposes (to monitor the quality and accuracy of the process) and for accountability purposes, to be able to demonstrate to supervisory authorities that disclosure requests are being handled in line with GDPR requirements. However, measures should be taken to protect the integrity and confidentiality of such records (in particular, taking into account that these records would contain both registrant and requestors' data). Also, the records should be subject to appropriate retention periods.

l. Data minimization, storage limitation and data accuracy: it would help to consider in advance (at the design stage) which data fields would need to be disclosed for each use case and to ensure that only necessary data fields are disclosed. Where it is possible to provide aggregate data, this option should be preferred: for example, where a Requestor requests the City field of 100 domain name registrations for statistical purposes, the SSAD could return the list of City fields without associating these to the corresponding domain name registration if this is not required for the purposes sought.

m. Individuals' rights: controller(s) need to address how individuals' rights requests will be fulfilled (for example, right of access, rectification, restriction, erasure) – that could be done by means of establishing a data rights policy. This point has been examined in the Liability memo (paras 3.13 et seq.) – we outline below some additional key considerations (albeit non exhaustive):
   - Right of access: the GDPR requires controller(s) to provide information on the recipients to whom personal data has been disclosed[46]; however, Member State laws may provide for exemptions to the right of access (for example, in the context of disclosure to law enforcement for crime detection purposes). As national legislation is not harmonised across EEA Member States, different rules might need to be considered.
   - The information provided under an access request might include personal data of third parties, e.g. the Requestor: in such case, the safeguards should include measures to review and decide whether it would be appropriate for such third party information to be withheld.
   - Other rights: Art. 19 GDPR requires controllers to notify recipients to whom personal data has been transferred of a request for rectification, erasure or restriction submitted by the data subject and the safeguards should provide for this.

[46] Art. 15(1)(c) GDPR – see also para 5.2.10 et seq. in this memorandum.

n. Engaging processors: where the controller(s) engage a service provider as a processor in the SSAD, they must ensure that they have carried out due diligence on their provider (for example, by means of an information security assessment) and that their contract with the provider includes appropriate data protection clauses as required by Art. 28 GDPR.

o. In addition to the above considerations, for use case 1 it would be appropriate to distinguish between LEA requests which create a legal obligation to disclose the requested information and requests the processing of which is subject to the controller(s)' discretion and judgement.