**Executive Summary:**

The EPDP Phase 2 team sent its first batch of questions to Bird & Bird on 29 August 2019. Bird & Bird answered this batch of questions in a series of three memos. [Memo 2](https://community.icann.org/download/attachments/117604842/ICANN-EPDP%20-%20Question%203%20-%2010th%20September%202019%5B1%5D.pdf?version=1&modificationDate=1568143539000&api=v2) was delivered on 10 September 2019 and analyzed questions related to how the legitimate interests “balancing test” required under GDPR Art 6(1)(f) (the "legitimate interests" legal basis for processing personal data) could be applied in a SSAD, either in highly automated fashion (Question A) or, if it is not possible to automate such a decision, then how the balancing test should be performed (Question B). The full questions are included in Annex A to this summary.

In response to Question A, Bird & Bird noted the following with respect to automation:

1. The highly-automated process described by the EPDP team could amount to solely automated decision making having a legal or similarly significant effect on the data subjects ("data subjects" here would be the targets of requests for nonpublic gTLD data).
2. This is generally is not permitted unless one of the limited legal bases/exemptions under GDPR Art. 22(1) would justify the disclosure. This is much narrower than GDPR Art. 6(1)(f). If GDPR Art. 22(1) applies, the legitimate interest legal basis (GDPR Art. 6(1)(f)) is therefore a somewhat moot/irrelevant point – there is a higher hurdle that needs to be cleared first: GDPR Art. 22.
3. It would be difficult for the SSAD, as proposed, to meet the GDPR Art. 22(1) exemptions; the SSAD must therefore be structured so it doesn’t fall into the scope of Article 22 in the first place.
4. To achieve this:
   1. It would be necessary to limit automatic access/disclosure to situations where there will be no "legal or similarly significant effects" for the data subject. The process for dealing with higher-risk requests should not be fully automated; some meaningful human involvement (at least, oversight) should be present; **or**
   2. Alternatively, the SSAD could potentially be structured so that it does not make a decision based on its automatic processing of personal data relating to targets of a request. For example, the SSAD could publish the categories of requests which will be accepted and ask Requestors to confirm that they meet the relevant criteria. By instead requiring *the Requestor* to conduct the necessary analysis and then certify the outcome to the SSAD, the SSAD would then arguably not make a decision (to release data) based on its own automated processing of personal data, so GDPR Art. 22 would not apply. However, relying on self-certification by Requesters perhaps creates scope for abuse of the system by Requesters, which (as previous answers explained) could mean liability for ICANN and the Contracted Parties.
5. As regards authentication of the Requester (as a distinct step from evaluating the grounds or other parameters of a request), Bird & Bird think it would certainly be possible to automate the process to authenticate the person making the request. It may also be possible to automate other aspects of the request process.”

In response to Question B, Bird & Bird:

1. set out the EU (WP29)'s official guidance on how the Art. 6(1)(f) legitimate interests balancing test should be conducted;
2. noted that if ICANN and Contracted Parties are joint controllers, they must both establish a legitimate interest in the processing. So far as Contracted Parties are concerned, it is likely that the relevant interest will be that of the third party, the Requester. ICANN, in contrast, may be able to establish its interest in the security, stability and resilience of the domain name system *as well as* the interest of the third party requester; and
3. provided a high level discussion of safeguards that could be deployed in order to further tip the scales in favour of the processing envisaged as part of the SSAD.

**1. Question A**

**Part A of the third question in essence asked whether GDPR Article 6(1)(f) (the "legitimate interests" legal basis for processing) would allow the SSAD to automatically process requests (at least in certain predefined categories), without requiring manual, request-by-request 1) verification that the request meets the relevant criteria for disclosure and 2) disclosure of the relevant registration data.**

*The SSAD could fall within the scope of GDPR Art. 22, rather than purely being concerned with GDPR Art. 6(1)(f)*

GDPR Art. 6(1)(f) permits automated processing *unless* this would amount to “automated individual decision-making” having legal or similarly significant effects for the data subject ("solely automated decision making"), which generally is not permitted unless one of the more limited legal bases/exemptions under GDPR Art. 22(1) would justify the disclosure.

While GDPR Article 22 states that a data subject has a "right not to be subject to" such a decision, in practice Article 22 has been interpreted by regulators as a general *prohibition* (i.e. there is no need for the data subject to object to such decision-making).

The process described by the EPDP team could amount to such automated decision-making affecting the target of a request (for instance, when law enforcement wants to bring a prosecution against individuals running unlawful websites).

If art.22 applies to the processing described by the EPDP, i.e. **if SSAD processing amounts to an automated individual decision having legal or similarly significant effects, it would not be permitted under GDPR Art. 6(1)(f) (the "legitimate interests" basis for processing).** Art. 22(1) sets out its own, more limited set of grounds on which Art. 22 decision-making can be based.

B&B advises that **it will be hard for the SSAD to meet the exemptions in Art. 22(1); so therefore, it’s necessary to make the SSAD fall outside the GDPR entirely**.

*Mitigation strategy 1: avoiding decisions if they might have "legal or similarly significant effects" for individuals whose data is disclosed*

One way to achieve this could be by limiting automatic access and disclosure to situations where there will not be “legal or similarly significant effects” for the data subject.

A decision to release data via the SSAD would not in itself have a "legal effect" on the data subject. The more relevant test for the SSAD is “similarly significant effects.” This means something similar to having legal effect -- something worthy of attention (e.g., significantly affect the circumstances, behavior or choices of the individuals concerned).[[1]](#footnote-1)

a legal or (company/organizational/institutional)

For decisions more likely to have a "significant effect", human review or oversight would be necessary. "Token" human involvement would not suffice. For the human review element to count, the controller must ensure meaningful oversight by someone who has the authority and competence to change the decision.

*Mitigation strategy 2: Avoiding SSAD designs that involve processing of personal data about the target of a request in order to decide whether to comply with the request*

It may also be possible to structure the SSAD so it doesn’t involve “a decision based solely on automated processing.” GDPR Article 22 requires the decision to be based on processing *of personal data.* If decisions are based on something other than personal data, GDPR Article 22 does not apply.

Therefore, rather than the SSAD requesting details from requesters (e.g. information about the target of the request, e.g. the registrant, and why their data is required), and then analyzing that information (automatically) in order to evaluate whether the relevant criteria for release of non-public registration data are met, the SSAD could instead publish the categories of requests which will be accepted, and ask requestors to confirm that they meet the relevant criteria. In this case, the SSAD would not process *personal data* about the target of the request, in order to reach a decision to release the data – so Article 22 would not apply.

As noted for earlier questions, parties involved in the SSAD have a responsibility to take "appropriate technical and organisational measures" to protect against the risk of misuse of the SSAD system by Requesters.

Any decision to rely on self-certification, rather than assessing requests, would therefore need to be balanced carefully against these risk mitigation obligations; this would likely narrow the occasions when this self-declaration approach could be used. Bird & Bird notes that under such a scheme, the SSAD could still 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 (i.e. it would not be used for automated decision-making).

**Question B**

In this question, **the EPDP team asks for guidance on how to perform the balancing test under 6(1)(f) (assuming it’s not possible to automate the steps described).**

Official guidance is that the balancing test should be divided into four steps:

1. Assess the interest which the processing meets
2. Consider the impact on the data subject
3. Undertake a provisional balancing test
4. Consider the impact of any additional safeguards deployed to prevent any undue impact on the data subject.

1. Assessing the controller’s legitimate interest

6(1)(f) says you can lawfully process if it is “necessary for the purposes of the legitimate interests pursued by the controller or a third party.”

There are three sub-elements to this: (i) legitimacy; (ii) existence of an interest; and (iii) necessity.

*Legitimacy*

It seems that “legitimacy” is not a high test -- WP29 said *“*an interest can be considered as legitimate as long as the controller can pursue this interest in a way that is in accordance with data protection and other laws.”

*""*

* B&B notes that if ICANN and Contracted Parties are joint controllers, they must both establish a legitimate interest in the processing. So far as Contracted Parties are concerned, it is likely that the relevant interest will be that of the third party, the requester. ICANN, in contrast, may be able to establish its interest in the security, stability and resilience of the domain name system as well the interest of the third party requester.
* “Interest” is not the same as “purpose.”
  + “Purpose” is the specific reason why the data is processed
  + “Interest” is the broader stake that a controller may have in the processing, or the benefit the controller derives, or that society might derive from the processing. (This also means that interests could be public or private; for example, in the case of actions to prevent trademark infringement, there could be a private interest for the person whose trademark has been infringed and a wider public interest in preventing a risk of confusion by the public. This factor could usefully be noted in the documentation of the balancing test.)
* Interest must be “real and specific”, not “vague and speculative.”
* At p.25, WP217 provides a non-exhaustive list of contexts in which legitimate interests may arise, including:
* "Exercise of the right to freedom of expression or information, including in the media and the Arts"
* Enforcement of legal claims
* Prevention of fraud, misuses of services,
* Physical security, IT and network security
* Processing for research purposes
* The EPDP suggests that potential SSAD safeguards could include requiring the requester to represent that it has a lawful basis for making the request and that it can "provide its lawful basis". However, where data will be released pursuant to art.6(1)(f), then it would be more helpful for the requester to confirm its *interest* in receiving the personal data.

*Necessity*

* With regard to necessity, B&B advises the proposed processing (disclosure) must be “necessary” for this interest.
  + - The CEJU Oesterreichischer Rundfunk case defines this as: *“…the adjective ‘necessary’…implies that a ‘pressing social need’ is involved and that the measure employed is ‘proportionate to the legitimate aim pursued’.”*
    - A UK Court of appeals likewise suggests that necessary means “more than desirable but less than indispensable or absolutely necessary.”
* B&B suggests that a relevant factor to consider for necessity could be whether a requester has tried to make contact with the individual in any other ways (although this may be inappropriate in the case of law enforcement requests).
* B&B notes that the SSAD proposes to ask requesters to confirm they are requesting only data that is necessary for their purpose.

2. Assessing the impact on the individual

* B&B says the EDPB suggests a range of factors to be considered when assessing the impact on the individual:
  + Assessment of impact. Consider the direct impact on data subjects as well as any broader possible consequences of the data processing (e.g., triggering legal proceedings).
  + Nature of the data. Consider the level of sensitivity of the data as well as whether the data is already publicly available.
  + Status of the data subject. Consider whether the data subject’s status increases their vulnerability (e.g., children, other protected classes).
  + Scope of processing. Consider whether the data will be closely held (lower risk) versus publicly disclosed, made accessible to a large number of persons, or combined with other data (higher risk).
  + Reasonable expectations of the data subject. Consider whether the data subject would reasonably expect their data to be processed/disclosed in this manner.
  + Status of the controller and data subject. ​ Consider negotiating power and any imbalances in authority between the controller and the data subject.
* It may be possible for the SSAD to take account of these factors, by identifying requests that would pose a high risk for individuals so that those requests receive additional attention.
* A classic risk methodology (looking at severity and likelihood) can be used in assessing risk.
* This is not a purely quantitative exercise; while a request's metrics (e.g. number of data subjects affected) is relevant, it is not determinative – a potentially significant impact on a single data subject should still be considered.

3. Provisional balance

Once legitimate interests of the controller or third party and those of the individual have been considered, they can be balanced. Ensuring other data protection obligations are met assists with the balancing but is not determinative (e.g., SSAD ensuring standard contractual clauses in place with requesters regarding adequate protection of data is helpful, because it perhaps reduces risk for individuals, but it is not determinative).

4. Additional safeguards

B&B reports that if it’s not clear how the balance should be struck, the controller can consider additional safeguards to reduce the impact of processing on data subjects.

These include, for example:

· Transparency

· Strengthened subject rights to access or port data

· Unconditional right to opt out

WP217, pp. 41-42, provides more details on safeguards that can help "tip the scales" in favour of processing (here, in favour of disclosures), in legitimate interests balancing test.

**Annex: Legal Question 3: legitimate interests and automated submissions and/or disclosures**

a) Assuming that there is a policy that allows accredited parties to access non-public WHOIS data through a System for Standardized Access/ Disclosure of non-public domain registration data to third parties ("SSAD") (and requires the accredited party to commit to certain reasonable safeguards similar to a code of conduct), is it legally permissible under Article 6(1)(f) to:

* + define specific categories of requests from accredited parties (e.g. rapid response to a malware attack or contacting a non-responsive IP infringer), for which there can be automated submissions for non-public WHOIS data, without having to manually verify the qualifications of the accredited parties for each individual disclosure request, and/or
  + enable automated disclosures of such data, without requiring a manual review by the controller or processor of each individual disclosure request.

b) In addition, if it is not possible to automate any of these steps, please provide any guidance for how to perform the balancing test under Article 6(1) (f).

For reference, please refer to the following potential safeguards:

* Disclosure is required under CP’s contract with ICANN (resulting from Phase 2 EPDP policy).
* CP’s contract with ICANN requires CP to notify the data subject of the purposes for which, and types of entities by which, personal data may be processed. CP is required to notify data subject of this with the opportunity to opt out before the data subject enters into the registration agreement with the CP, and again annually via the ICANN- required registration data accuracy reminder. CP has done so.
* ICANN or its designee has validated the requestor’s identity, and required that the requestor:
  + represents that it has a lawful basis for requesting and processing the data,
  + provides its lawful basis,
  + represents that it is requesting only the data necessary for its purpose,
  + agrees to process the data in accordance with GDPR, and
  + agrees to standard contractual clauses for the data transfer.
* ICANN or its designee logs requests for non-public registration data, regularly audits these logs, takes compliance action against suspected abuse, and makes these logs available upon request by the data subject.

1. According to official guidance, the following are classic examples of decisions that could be sufficiently significant: (i) decisions that affect someone’s financial circumstances; (ii) decisions that affect access to health services; (iii) decisions that deny employment opportunities or put someone at a serious disadvantage; (iv) decisions that affect someone’s access to education. [↑](#footnote-ref-1)