Bird & Bird

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

TO:	ICANN GNSO Expedited Policy Development Process on the Temporary Specification for gTLD Registration Data team ("EPDP team")
FROM:	Ruth Boardman & Nora Santalu, Bird & Bird LLP
DATE:	10th September 2019
RE:	"Batch 1" of GDPR questions regarding a System for Standardized Access/Disclosure ("SSAD")

Question 3, legitimate interests and automated submissions and/or disclosures

The EPDP team has asked the following questions:

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. QUESTION A

1.1 Question a) describes the processing which will be undertaken through the SSAD, namely, 1) receiving requests for access to non-public registration data and verifying that the request meets the relevant criteria for disclosure and 2) disclosing the relevant registration data. Article 6(1) (f) will be applicable, in some cases, when the relevant party(ies) disclose non-public registration data as part of the SSAD. Accordingly, question a) asks if it is legally permissible under art.6(1)(f) to automate the processing described above.

Art.6(1)(f) permits entirely solely automated processing unless this would amount to "automated individual decision-making"

1.2 The EPDP team describes a situation in which there would be no human involvement in the decision of whether or not to release non-public domain registration data to third parties. The European Data Protection Board ("EDPB") has adopted *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (revised and adopted by the Article 29 Working Party on 6 February 2018 and endorsed by the EDPB) ("WP251"). In WP251, the EDPB defines "solely automated decision making" as "*the ability to make decisions by technological means without human involvement*" (p.8). The process described by the EPDP team could amount to solely automated decision making.

1.3 WP251 notes that the GDPR distinguishes between:

1.3.1 Profiling and solely automated decision making; and

1.3.2 "automated individual decision-making", as defined in art.22, which includes, but is not limited to, automated individual decision-making based on profiling.

1.4 The distinction is significant because, as the EDPB notes[1]:

"*Automated decision-making defined in Article 22(1) is only permitted if one of the exceptions .... applies. The following lawful bases for processing* [including 6(1)(f)] *are relevant for all other automated individual decision-making and profiling"*[2] (emphasis added)

"*The controller's "legitimate interest" cannot render profiling* [or automated decision making] *lawful if the processing falls within the Article 22(1) definition"*[3] and further stresses that *"additional safeguards and restrictions apply in the case of solely automated decision-making, including profiling, defined in Article 22(1)."*[4]

1.5 Accordingly if art.22 applies to the processing described by the EPDP, such that it amounts to an automated individual decision, it would not be permitted under art.6(1)(f).

It will be difficult for the SSAD to meet the exemptions in art.22(1); it will, therefore, be necessary to limit automatic access/disclosure to situations where there will not be "*legal or similarly significant effects*" for the data subject; alternatively the SSAD could potentially be structured so that the release does not amount to a "decision based on automatic processing"

1.6 Article 22 applies to:

[1] As the quotations below show, the EDPB uses the terms automated decision making, automated individual decision making and solely automated decision making inconsistently. In this note, we have followed art.22 itself in referring to processing to which that article applies as "automated individual decision-making" and other types of entirely automated decisions as "solely automated decision making".

[2] WP251, p.12

[3] WP251rev.01 "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", see footnote 19.

[4] WP251rev.01 "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679" ", p.9.

"*a decision based solely on automated processing, including profiling, which produces legal effects concerning* [the data subject] *or similarly significantly affects him or her*".

A data subject (here the registrant, where the registrant is a natural person, or the point of contact at a registrant which is a non-natural person), has the right "*not to be subject to*" such a decision. Article 22(2) sets out situations where this provision does not apply. Recital 71 notes that automated individual decisions "*should be allowed"* in line with these exemptions: the implication being that on other occasions the processing is not allowed. As WP251 notes (pp.19 &.23), there is no need for a data subject to object to this type of processing; Art.22 sets out a general prohibition on automated individual decision-making. We have set out commentary on the exemptions to Art.22 in the Appendix to this note. As will be seen from the Appendix, it is likely to be difficult for the SSAD to satisfy the exemptions. It is, thus, important to ensure that the SSAD does not amount to an automated individual decision.

1.7 As an initial point, we note that any automated decision on whether or not to recognise a party as accredited would not be affected by this provision - on the basis that the registrant/ registrant's point of contact is not the subject of that decision: rather the party requesting access is the subject of the decision.

1.8 Most automated individual decision-making is likely to involve profiling, defined at art.4(4) of the GDPR as "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person…*". The processing described by the EPDP team will not involve profiling relating to the domain name registrant or contact. However, as mentioned at 1.3.2, art.22 is not limited to profiling, and covers other types of solely automated decisions if they have legal or similarly significant effect. Here, WP251 gives the example of imposing speeding fines – which is an automated decision-making process, but which does not involve profiling (p.8).

1.9 On whether a decision has "legal effect", WP251 states that:

"*A legal effect requires that the decision, which is based on solely automated processing, affects someone's legal rights, such as the freedom to associate with others, vote in an election, or take legal action. A legal effect may also be something that affects a person's legal status or their rights under a contract. Examples of this type of effect include automated decisions about an individual that result in:*

- *cancellation of a contract;*
- *entitlement to or denial of a particular social benefit granted by law, such as child or housing benefit;*
- *refused admission to a country or denial of citizenship."*[5]

A decision to release information via the SSAD is would not in itself have legal effect on the data subject.

1.10 On "*similarly significantly affects him or her*", WP251 states that:

"*… the threshold for significance must be* <u>*similar*</u> *to that of a decision producing a legal effect…. For data processing to significantly affect someone the effects of the processing must be sufficiently great or important to be worthy of attention. In other words, the decision must have the potential to:*

- *significantly affect the circumstances, behaviour or choices of the individuals concerned;*
- *have a prolonged or permanent impact on the data subject; or*

[5] WP251rev.01 "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679"", p.21.

- *at its most extreme, lead to the exclusion or discrimination of individuals.*

It is difficult to be precise about what would be considered sufficiently significant to meet the threshold, although the following decisions could fall into this category:

- *decisions that affect someone's financial circumstances, such as their eligibility to credit;*

- *decisions that affect someone's access to health services;*

- *decisions that deny someone an employment opportunity or put them at a serious disadvantage;*

- *decisions that affect someone's access to education, for example university admissions."*[6]

1.11 It may be possible to determine categories of requests where the release would not have "similarly significant" effect on the individual. By way of examples, it seems likely that the release of administrative contact details for non-natural registrants in connection with rapid response requests for malware attacks, or in connection with potential IP infringements, would not have a "similarly significant effect". In other situations, disclosure of registrant data about a natural person (for example, in connection with a serious offence) may be much more likely to have a "similarly significant effect". Considerable care would need to be taken over such analysis.

1.12 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.

1.13 As noted in our response to Qs 1 & 2, those involved in the SSAD have a responsibility, under Art.32, to take account of the risks of unlawful or unauthorised access to personal data and to take "appropriate technical and organisational measures" to protect against this risk. This would extend to anticipating misuse of the SSAD process. Any decision to rely on self-certification, rather than assessing requests made, would therefore need to be balanced carefully against obligations under Art.32 and would likely narrow the occasions when this self-declaration approach could be used.

1.14 Lastly, we note that, in its question, the EPDP has sought to distinguish between automated verification of requests and automated disclosure of data. We have considered if it is possible to split the processing in this way, such that processing that does not lead to a decision which has similarly significant effects could be entirely automated. As noted at 1.7 above, we 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. However, if all aspects of the review process were automated, it is difficult to see what level of discretion would be left for human review at the point of disclosure, with the result that the decision to qualify the request would, in itself, become a decision which has similarly significant effect.

1.15 From a similar perspective, the EDPB notes that it is not possible to avoid the provisions of art.22 by interposing notional human involvement:

"*To qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone*

[6] WP251rev.01 "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679"", p.21.

who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data."[7]

If the person(s) responsible for the SSAD ensured that there was this element of meaningful human review of the overall decision to release data, then the provisions of art.22 would, of course, not apply, as the decision would not be based "*solely"* on automated processing.

Conclusion: Automated individual decision-making

1.16 Article 22 of the GDPR prohibits decisions based solely on automated processing of personal data which have legal or similarly significant effect. While there are exemptions to this provision it is likely to be difficult for the SSAD to meet these. The SSAD will, therefore, need to be structured so that it does not fall within the scope of Article 22. This will restrict its use to situations where the release of non-public registrant has more minor consequences for the individuals concerned.

2. QUESTION B

2.1 In question b) the EPDP team asks for guidance on how to perform the balancing test under art.6(1)(f).[8]

2.2 The Article 29 Working Party issued guidance on performing the balancing test in its *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (WP 217). The balancing test required under the GDPR is identical to that under the Directive, so the guidance is still relevant. This suggests that the balancing test should be split into four steps (p.33) : 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. We have commented on each of these steps below.

Assess the controller's legitimate interest

2.3 Article 6(1)(f) provides that processing will be lawful if it is "*necessary for the purposes of the legitimate interests pursued by the controller or by a third party…"*. The first element in the balancing test is, therefore, to establish the interest being pursued by the controller or by a third party; to confirm that this interest is legitimate; and to confirm that the processing is necessary for this purpose.

Establishing the interest in the processing

2.4 WP 217 notes (p.24) that:

"*The concept of 'interest' is closely related to, but distinct from, the concept of 'purpose'… 'purpose' is the specific reason why the data are processed: the aim or intention of the data processing. An interest, on the other hand, is the broader stake that a controller may have in the processing, or the benefit that the controller derives, or that society might derive – from the processing"*.

WP29 includes an example to clarify the distinction:

"a company may have an interest in ensuring the health and safety of its staff working at its nuclear power plant. Related to this, the company may have as a purpose the implementation of specific access control procedures which justifies the processing of certain specified personal data in order to help ensure the health and safety of staff".

[7] WP251, p.21

[8] The question asks for guidance on how to perform the balancing test if it not possible to automate any of the steps described. For the avoidance of doubt, we wanted to note that the balancing test must still be carried out even if some of the steps described are automated.

To take an example more relevant to the EPDP, a relevant interest here may be ensuring availability of services, and the purpose may be taking action against a denial of service attack.

2.5 As art.6(1)(f) makes clear, the interest can either be that of the controller responsible for the processing or that of a third party. It is possible that ICANN and the CPs may be joint controllers in respect of some aspects of the SSAD, in which case each will need to establish a legitimate interest in the processing.[9] So far as CPs are concerned, it is likely that the relevant interest will be that of the third party, the requester. Given ICANN's mission is to contribute to the security, stability and resilience of the domain name system, ICANN may well be able to establish its own legitimate interest in disclosure as well as pointing to the interest of the requester.

2.6 WP217 notes that the interest should be *"real and present*" as opposed to being "*vague and speculative*" (p.24). The controller must also determine that the interest is "legitimate" – which WP217 notes could include a broad range of interests, ranging from the trivial to the compelling. According to WP29 "*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. In other words, a legitimate interest must be 'acceptable under the law'*" (p.25) . It seems that "legitimacy" is not a high test – although the nature of the interest pursued can be relevant when this is balanced against the impact of the processing on the individual (p.24). In this regard, it is useful to note whether the interest pursued is purely private, or if there is also a wider public or community interest. Both may often be relevant to those operating the SSAD – 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.

2.7 At p.25, WP217 provides a non-exhaustive list of contexts in which legitimate interests may arise:

"*exercise of the right to freedom of expression or information, including in the media and the arts*

Conventional direct marketing ...

Unsolicited non-commercial messages...

Enforcement of legal claims...

Prevention of fraud, misuses of services, or money laundering

Employee monitoring for safety or management purposes

Whistle-blowing schemes

Physical security, IT and network security

Processing for historical, scientific or statistical purposes

Processing for research purposes (including marketing research)".

Recital 49 of the GDPR expands on the brief reference to security, noting, by way of example, that this could include preventing malicious code distribution and stopping denial of service attacks. We anticipate that the interests underlined above would be relevant to many of those making requests to the SSAD.

2.8 The EPDP suggests that potential 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

[9] See note on Qs 1 & 2.

basis". 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"

2.9 The proposed processing (disclosure) must be "necessary" for this interest. The CJEU case of *Oesterreichischer Rundfunk*[10] concludes that:

> ".. *the adjective' necessary' ... implies that a 'pressing social need' is involved and that the measure employed is 'proportionate to the legitimate aim pursued'.*

A gloss provided by the UK Court of Appeal can be helpful, which suggests that this means "*more than desirable but less than indispensable or absolutely necessary"*.[11] WP217 does not provide any detailed guidance on this. This may vary by the nature of the requester. For example, in the case of requests by rightsholders, a relevant factor could be whether they have already tried to make contact with the relevant person in other ways. This test may clearly be inappropriate for requests from law enforcement authorities if it would pose a risk to an ongoing investigation. We note that the SSAD proposes to ask requesters to confirm that they are only requesting data which is necessary for their purpose.

Assess the impact on the individual

2.10 WP217 suggests a wide range of factors to be considered – and specifically notes that the interests of an individual suspected of wrongdoing must also be taken into account (p.30):

- Both positive and negative impact on the individual (with impact being considered in wide terms, extending to emotional impact) – disclosure of registration data could presumably trigger adverse consequences by way of legal proceedings (civil and criminal) and associated emotional distress.
- The nature of the data to be disclosed and whether any of it is special category data – the data to be disclosed pursuant to the SSAD would not, of itself, amount to special category data. However, in certain situations, this could be relevant – for example, where a website discusses the political opinions, health, or sexual life of the registrant.
- The way the data is processed – in particular whether there will be a wide disclosure (presumably not the case here) and whether data will be combined with other data (a more significant risk).
- The reasonable expectations of the individual and whether they could expect this processing given the nature of the relationship between controller and data subject. We note that the safeguards include provision of information to individuals about the SSAD both initially and on an annual basis.
- The status of the individual and any particular vulnerability – for example, WP217 suggests that special care may be needed for vulnerable groups such as children, those with mental health difficulties, or asylum seekers.

2.11 It may be possible for the SSAD to take account of these factors – for example, by seeking to identify requests which would pose a particularly high risk for individuals, because of the likely impact to the individual due to the nature of the proceedings, or the data, or their vulnerable status, so that additional attention could be given to such requests.

2.12 WP217 suggests (p.38) that a classic risk methodology (looking at severity and likelihood) is used in assessing risk. Although it also notes that this is not a purely quantitative exercise, nor

[10] Joined cases C-465/00, C-138/01, C-139/01, 2003

[11] *Michael Cooper v National Crime Agency* [2019] EWCA Civ.16, approving the interpretation of the first instance judge.

is the number of data subjects determinative – a potentially significant impact on a single data subject should be considered.

Provisional balance

2.13 Once the legitimate interests of the controller or third party and those of the individual(s) have been considered, then they can be balanced. The Article 29 Working Party notes that the fact that other data protection obligations are met will assist – but does not mean that the processing can necessarily proceed. So the fact that – by way of example, the SSAD will ensure that standard contractual clauses are in place with recipients where this is required to ensure adequate protection for personal data, is helpful but not determinative.

Additional safeguards

2.14 In the event that it is not clear which way the balance should be struck, then the controller may consider additional safeguards to reduce the impact of processing on data subjects. WP217 contains a list of possible safeguards (pp. 41 -42), such as transparency, strengthened subject rights to access or port data, or an unconditional right to opt-out, requirements for functional separation for those accessing data (for example, a researcher accessing data should not be able to use the data to take decisions about the individual), anonymization or aggregation techniques.

2.15 The suggestions in relation to aggregation, anonymization and unconditional opt-outs would, we assume, undermine the purpose of the disclosure. Suggestions of enhanced individual rights (for example in relation to portability) would also not seem to mitigate the risk to individuals. The reference to commitments in relation to re-use of the data for some requests (particularly research) could potentially be implemented. There are already plans for extensive transparency commitments.

Appendix: exemptions from Article 22(1) GDPR

Art.22 of the GDPR prohibits automated individual decision-making unless the decision is:

- necessary for the performance of a contract,
- authorised by Union or Member State law, or
- based on data subject's explicit consent.

Necessary for the performance of a contract (art.22(2)(a))

1. For this exemption to apply, both the processing *and* the solely automated nature of the processing must be necessary for entering into, or performance of, a contract between the data subject and a data controller.[12] Accordingly, the condition could never apply where the personal data requested relates to a registrant which is a legal (rather than a natural) person.

2. As the EPDP team is aware, data protection authorities interpret the provision strictly. On 9th April 2019, the EDPB issued draft *Guidelines on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects* (no reference number yet issued). Article 6(1)(b) applies where "*processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract*". The core requirement of contractual necessity is the same in both art.22(2)(a) and art.6(1)(b). On this, the draft Guidelines (p.8) state that:

   "*.. it is required that the processing is objectively necessary for a purpose that is integral to the delivery of that contractual service to the data subject... The controller should be able to demonstrate how the main object of the specific contract with the data subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur... A contract cannot artificially expand the categories of personal data or types of processing operation that the data controller needs to carry out for the performance of the contract...*" (emphasis added).

3. Disclosure of registration data to requesters – whether in an entirely automated manner or not – cannot be described as objectively necessary for a purpose that is integral to the registration of the domain name.

Authorised by Union or Member State law (art.22(2)(b))

4. Art.22(2)(b) permits automated individual decision-making if the decision is "*authorised by Union or Member* State *law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests*".

5. Relevant controller(s) (either the CPs or ICANN) may be subject to EU or Member State law permitting automated individual decision-making. Unless an EU law[13] were to permit the automated individual decision-making foreseen by the SSAD, any attempt to rely on this provision would require consideration of the laws of Belgium (if ICANN's Belgian establishment is relevant) or the Member State law(s) applicable to the particular CP (assuming the CP is the controller). This would require further analysis and would add complexity to the SSAD, as it would need to be able to distinguish between the laws applicable to different requests.

6. Art.22(2)(b) provides that any relevant law must "*lay down suitable measures to safeguard the data subjects rights and freedoms*". These safeguards may also be problematic or incompatible with the proposed operation of the SSAD. By way of example, in the UK, the UK's Data Protection Act 2018 s.14 contains a general enabling provision stating that any decisions which are "*required or authorised by law*", and which are not otherwise permitted by art.22(2)(a) (contractual necessity) or (c) (consent) are "*qualifying significant decisions*" for the purposes of art.22(2)(b)).

[12] WP251, p.23

[13] Such as an implementing act under the Cybersecurity Act

However, the safeguards require the controller to notify the data subject as soon as possible that a decision has been taken, at which point the data subject has up to one month to require the controller to reconsider the decision, with significant operational implications for any urgent requests.

Explicit consent (art.22(2)(c))

7. Automated individual decision-making can take place if the decision is based on the data subject's explicit consent. Recital 43 notes that *"in order to ensure that consent is freely given,* consent *should not provide a valid ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller.."* Further, per. Recital 42, "*consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment"*. It would, therefore, have to be clear to the data subject that consent is entirely voluntary, could be given or withheld (and later withdrawn) at his or her entire discretion. It is difficult to see how this would be practicable for the SSAD.

Member state derogations

8. Article 23 of the GDPR allows Member States to restrict provisions of the GDPR, including art.22, in certain situations. It is possible that some Member States may have introduced restrictions which could be applicable to the SSAD. 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. Again, this would require further analysis on a Member State specific level and would add to the complexity of the SSAD.

Safeguards

9. The SSAD may be able to facilitate entirely automated requests for disclosure of registration data if it can show that the decisions to release the data are permitted by Union or Member State law. As noted above, any such laws would need to set out suitable measures to safeguard the data subject's rights and freedoms. Recital 71 notes that the safeguards "*should include specific* information *to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision"*. WP251 underlines that "*This emphasises the need for transparency about the processing. The data subject will only be able to challenge a decision or express their view if they fully understand how it has been made and on what basis"* (p.27). The initial and annual notice and opt-out process suggested by the EPDP would not be sufficient: an individual would be given general notice that an automated process may be used, but would not know that a decision has actually been taken on this basis and, unless an individual was aware of this, he or she would not be in a positon to take advantage of the safeguards required by the GDPR.

10. We assume that any case-by-case notice process would undermine the benefits of the SSAD. WP251 also suggests additional safeguards which should be considered for automated individual decision-making. If the EPDP team considers that automated individual decision-making is feasible, notwithstanding the difficulties outlined in this note, then we can provide further details.