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

MEMORANDUM

To: Internet Corporation for Assigned Names and Numbers (ICANN), EPDP Team
From: Ruth Boardman & Katerina Tassi, Bird & Bird LLP
Date: 9 April 2020
Subject: Advice on Accuracy Principle under the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**"): follow up queries on "Legal vs. Natural" and "Accuracy" memos

---

EXECUTIVE SUMMARY

This document examines further considerations in relation to the Accuracy Principle (the parties with the obligation to comply with this principle, persons that have the standing to invoke it, and the basis on which data accuracy is to be assessed). It sets out the factors to be considered when assessing data accuracy and provides recommendations of measures to enhance the accuracy of registration data held by contracted parties.

Parties subject to Accuracy Principle and "relevant parties"
The obligation to comply with the GDPR's Accuracy Principle lies with the controller(s). References to "relevant parties" in the Accuracy and the Legal vs. Natural memos were to the relevant controller(s) of WHOIS data.

Parties having the right to invoke the Accuracy Principle
The GDPR provides for a range of remedies: complaints to supervisory authorities, judicial remedies and right to compensation from a controller or processor. Data subjects (and where allowed by national law, their representatives) have the right to exercise all remedies set forth in the GDPR. In some instances, these rights may also be exercised by other –natural or legal- persons, for example, those affected by the decision of a supervisory authority or those suffered damage as a result of an infringement of the GDPR.

Interests of various parties when considering accuracy
The purpose for which personal data is processed is relevant to determining the measures required to ensure data accuracy. The data subject's interests must be taken into account when assessing data accuracy. In some circumstances, the controller's interests will also be relevant. Although there are a few references to rights of "others" in ICO's accuracy guidance, this point is not illuminated further in our review of guidance, case law or literature. Given the lack of guidance, we do not recommend placing too much emphasis on this point.

Reasonable measures for data accuracy
The Accuracy Principle has not been extensively examined in literature and case law and references to it are limited. The reasonable and appropriate character of accuracy measures should be considered in the light of the GDPR's risk-based approach, taking into account, among other things, the purpose and impact of processing. A list of suggested accuracy measures is set out in this document.

Background

The current approach in respect of registration data is to treat all registrations as if they may contain personal data. However, seeing that non-personal registrants make up a considerable portion of registrants, one proposal is to distinguish non-personal registrants from those that provide personal data by allowing registrants to self-identify as legal persons at the time of registration. Under this approach, registration details would be made publicly available by default for non-personal registrants and contracted parties would rely on this self-identification when deciding whether to redact the registration data.

We have previously examined data protection considerations relating to registrants' incorrect self-identification in advice provided in the Accuracy and Legal vs. Natural memos. By way of follow up to these memos, the EPDP Legal Committee has now provided the below set of further questions.

Questions presented

Question 1

1.a Who has standing to invoke the Accuracy Principle? We understand that a purpose of the Accuracy Principle is to protect the Data Subject from harm resulting from the processing of inaccurate information. Do others such as contracted parties and ICANN (as Controllers), law enforcement, IP rights holders, etc. have standing to invoke the Accuracy Principle under GDPR? In responding to this question, can you please clarify the parties/interests that we should consider in general, and specifically when interpreting the following passages from the prior memos:

- Both memos reference "relevant parties" in several sections. Are the "relevant parties" limited to the controller(s) or should we account for third-party interests as well?
  - "There may be questions as to whether it is sufficient for the RNH or Account Holder to confirm the accuracy of information relating to technical and administrative contacts, instead of asking information of such contacts directly. GDPR does not necessarily require that, in cases where the personal data must be validated, that it be validated by the data subject herself. ICANN and the **relevant parties** may rely on third-parties to confirm the accuracy of personal data if it is reasonable to do so. Therefore, we see no immediate reason to find that the current procedures are insufficient." (emphasis added) (Paragraph 19 – Accuracy)

  - "In sum, because compliance with the Accuracy Principle is based on a reasonableness standard, ICANN and the **relevant parties** will be better placed to evaluate whether these procedures are sufficient. From our vantage point, as the procedures do require affirmative steps that will help confirm accuracy, unless there is reason to believe these are insufficient, we see no clear requirement to review them." (emphasis added) (Paragraph 21 - Accuracy)

  - "If the **relevant parties** had no reason to doubt the reliability of a registrant's self-identification, then they likely would be able to rely on the self-identification alone, without independent confirmation. However, we understand that the parties are concerned that some registrants will not

understand the question and will wrongly self-identify. Therefore, there would be a risk of liability if the **relevant parties** did not take further steps to ensure the accuracy of the registrant's designation." (emphasis added) (Paragraph 17 – Legal v. Natural)

1.b Similarly, the Legal vs. Natural person memo refers to the "importance" of the data in determining the level of effort required to ensure accuracy. Is the assessment of the "importance" of the data limited to considering the importance to the data subject and the controller(s), or does it include the importance of the data to third-parties as well (in this case law enforcement, IP rights holders, and others who would request the data from the controller for their own purposes)?

- "As explained in the ICO guidance, "The more important it is that the personal data is accurate, the greater the effort you should put into ensuring its accuracy. So if you are using the data to make decisions that may significantly affect the individual concerned or others, you need to put more effort into ensuring accuracy." (Paragraph 14 – Legal vs. Natural)

Analysis

1. Under the first limb (1.a) of this question, we examine:
   (i) Which parties bear the obligation to comply with the Accuracy Principle under the GDPR (para 2 below);
   (ii) Which parties are meant by the reference to "relevant parties" (para 3); and
   (iii) When considering the Accuracy Principle, which parties have the right to initiate an administrative or legal procedure (paras 4-8).

2. Obligation to comply with the Accuracy Principle: By way of a reminder, we note that the Accuracy Principle set out in Article 5(1)(d) GDPR provides that personal data "*shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*". The obligation to comply with the Accuracy Principle lies with the controller(s) of the relevant personal data. Pursuant to Article 5(2) GDPR, the controller shall be responsible for (and be able to demonstrate compliance with) the principles relating to processing of personal data, including the Accuracy Principle.

3. "Relevant parties": References to "*relevant parties*" in the Accuracy and the Legal vs. Natural memos indicate the parties which are controllers in respect of WHOIS data. As discussions around the controller status of contracted parties were ongoing at the time when these memos were drafted, we used the term "relevant parties" to refer to those parties that act as controllers of WHOIS data.

4. Invoking the Accuracy Principle: The GDPR provides for two sets of remedies in relation to the infringement of its provisions (including the Accuracy Principle):
   (a) enforcement action by supervisory authorities; and
   (b) judicial remedies and compensation.

Each remedy is available to different types of parties; hence, the remedy used in each case will determine whether or not a party has the standing to invoke the Accuracy Principle. This is examined in more detail below.

5. Enforcement action by supervisory authorities

(i) Right to lodge a complaint with a supervisory authority[1]. This right to complain is reserved to data subjects who consider that the processing of their personal data infringes the GDPR. If the authority does not handle the data subject's complaint, the latter has the right to an effective judicial remedy against such authority[2].

It is worth noting that in practice, parties other than the data subject may also be able to raise a data protection issue with a supervisory authority. Part of a supervisory authority's tasks is to monitor and enforce the application of the GDPR as well as to conduct investigations on the application of the GDPR[3]. In this respect, each supervisory authority has investigative powers which include requesting information from controllers or processors, carrying out investigations and notifying controllers or processors of an alleged infringement of the GDPR. On this basis, it follows that if a party other than the data subject draws the attention of a supervisory authority to an alleged infringement of the GDPR (such as non-compliance with the Accuracy Principle), then the supervisory authority would have the power to examine such allegation further and take the steps it considers necessary in line with its investigative and corrective powers. Hence, although third parties other than data subjects are not granted the right in the GDPR to lodge a formal complaint with a supervisory authority, it may still be possible for them to raise with the authority issues relating to the compliance with the GDPR. In some countries, national legislation might as well provide or allow for this[4].

6. Judicial remedies and compensation

(i) Right to an effective judicial remedy against a supervisory authority: Where a supervisory authority issues a legally binding decision, the GDPR establishes the right to an effective judicial remedy against such decision: this is reserved to each natural or legal person concerned by the authority's decision. Although a person concerned by a decision would reasonably be either the data subject and/or a party having the status of controller or processor (as these categories of parties would be involved in proceedings before a supervisory authority), the wording of the GDPR suggests that this could be

[1] Article 77 GDPR.

2 Article 78(2) GDPR.

[3] Article 57(1)(a) & (h) GDPR.

[4] For example, the Belgian Act establishing the Data Protection Authority provides that "*anyone*" may submit a complaint or request to the Authority, thus recognising a broader scope than the GDPR. Also, in Germany, the "petition right" established in the German constitution, allows individuals to submit requests to any administrative governmental body; in such case, a supervisory authority would need to consider the request and provide a meaningful response. In Spain, the legal provisions regulating the procedures followed by the Spanish supervisory authority ("AEPD") do not restrict the lodging of complaints to data subjects and the AEPD has traditionally been willing to receive complaints from any person.

wider and could include any other persons affected by the authority's decision (see relevant analysis under point (iii) below).

(ii) Right to an effective judicial remedy against a controller or a processor[5]: This right is reserved to data subjects, where they consider that their rights under the GDPR have been infringed as a result of the non-compliant processing of their personal data. Unlike the right to complain to the supervisory authority, other parties would not be in a position – even unofficially – to initiate such proceedings; and

(iii) Right to compensation from a controller or a processor[6]: Article 82 GDPR provides that "*any person*" who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the controller or processor for the damage suffered. The GDPR does not further specify which parties are entitled to compensation; however, the different wording used in Article 82 GDPR - compared to the rights examined above- indicates that there is no limitation to data subjects and a –natural or legal- person that is not a data subject would be in a position to bring a claim for compensation, as appropriate[7]. The principal element for a person to qualify for compensation is to have suffered damage. On this basis, theoretically, other parties such as IP rights holders could potentially claim compensation for damages resulting from an infringement of the Accuracy Principle; however, in practice, depending on the circumstances it may be challenging for such third parties to establish that they have suffered damage as a result of controllers' non-compliance with the Accuracy Principle. Based on literature searches at CJEU level and in the UK, Germany, France, Belgium and Spain, we do not believe this has yet been tested in practice.

7. Representative bodies: For the sake of completeness, we note that – where provided for by EU Member State law – data subjects have the right to mandate a representative body to exercise on their behalf the rights examined under para 5 and 6 above[8]. Such representative body shall be any not-for-profit body, organization or association which is properly constituted according to EU Member State law, has statutory objectives which are in the public interest and is active in the field of data protection.

8. The table below summarises the available remedies under the GDPR and the parties entitled to each remedy[9]:

[5] Article 79 GDPR.
[6] Article 82 GDPR.
[7] *Rosemary Jay*, Guide to the General Data Protection Regulation, A Companion to Data Protection Law and Practice, p. 294. We note however that in Germany there is controversy around this point, with part of the literature suggesting that the right to compensation is reserved to data subjects, and another part suggesting that it applies to both natural and legal persons and a smaller part considering it applies to natural persons only.
[8] Article 80 GDPR.
[9] We have not considered any possible liability arising from contractual arrangements (for example, by virtue of a data sharing agreement between a registrar and a law enforcement agency containing accuracy-related provisions) or wider issue of tortious liability outside of data protection.

Remedy	Parties			
	Data Subject	**Representatives** (where provided for by member state law)	**Controller/ Processor**	**Other parties**
Complaint with a supervisory authority	✓	✓		✗* *unofficial complaints from other parties may still be possible
Judicial remedy against a supervisory authority	✓	✓	✓	✗
Judicial remedy against a controller/processor	✓	✓		✗
Compensation	✓	✓	✓	✓

9. Parties' interests when considering data accuracy: Under the second limb of this question (1.b), we examine the element of "*importance*" of the accuracy of personal data and whose interests must be taken into account in the Accuracy Principle (paras 10-12). Considering the context within which the ICO refers to the importance of personal data being accurate, it is clear that the notion of "importance" is associated with the purpose of processing[10] and the consequences that the processing may have for individuals.

10. The most obvious person whose interests must be taken into account when considering data accuracy, therefore, is the data subject. Existing case law, guidance and examples in literature focus on the data subject's interests[11]. This is also in line with the GDPR's objective to protect the fundamental rights and freedoms of individuals[12].

11. The purposes pursued by the controller (and the controller's commercial interests) would also be relevant when examining accuracy. The ICO's accuracy guidance includes the example of pre-employment checks in order to verify information about a candidate's qualifications. In such a case the independent verification

[10] The significance of the purpose of processing has been recognised in case law (for example, in the Nowak case (C-434/16), the Court considered that "*the assessment of whether personal data is accurate and complete must be made in the light of the purpose for which that data was collected*"), in literature (e.g. BeckOK DatenschutzR/Schantz, 31. Ed. 1.2.2019, DS-GVO Art. 5, Rn. 27-29) and is also supported in the Explanatory Memorandum on OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("OECD Explanatory Memorandum"), which notes in respect of the accuracy principle: "*The requirements in this respect are linked to the purposes of data, i.e. they are not intended to be more far-reaching than is necessary for the purpose for which the data are used. […] The "purpose test" will often involve the problem of whether or not harm can be caused to data subjects because of lack of accuracy, completeness and up-dating*".

[11] See for example reference in OECD Explanatory Memorandum above. Also, by way of non-exhaustive examples in guidance, the ICO's guidance on the use of live facial recognition technology in public spaces examines accuracy under the prism of the impact to individuals, suggesting that inaccurate data matching has "*the potential to cause unwarranted damage and distress to individuals*".

[12] Article 1(2) GDPR.

checks (e.g. by means of third party references) to ensure accuracy are not carried out for the benefit of the data subject. An employee who does not have the qualifications they purport to have would harm the employer's commercial interests. In these circumstances, the controller would have an interest to ensure the accuracy of the data presented to it and this would be independent of the interests of the data subject.

12. When considering the relevance of the "purpose" of processing, we note that the European Data Protection Board ("EDPB") has previously emphasised that the purposes of third parties are not the same as the purposes for which ICANN and contracted parties process personal data[13]. This comment could possibly be relevant to the determination of what data is needed in terms of adequacy. The ICO guidance, however, also contains the example of an employer checking whether a candidate for a role as a driver has the necessary licence required. In this case, an employee who does not have the qualifications they purport to have would harm the employer's commercial interests and would also pose a risk to public safety.

13. We have found little coverage of other parties' interests. It is implicit in the ICO example above. There is also brief explicit acknowledgement by ICO that other parties may be affected by the processing of inaccurate personal data[14]; however, this reference to other parties is one of the few occasions where the possibility of wider interests is acknowledged and the ICO does not clarify what is meant by other parties, nor does it provide any examples in this respect. To our knowledge, there is no specific guidance or case law illuminating this point.

14. To conclude, we think that the accuracy principle could, *in principle*, extend so as to require controllers to consider the interests of persons other than the data subject and the data controller. However, given the almost complete lack of guidance on this, we think there is considerable risk in putting too much weight on this point. Based on existing guidance, we do not think that the principle would extend to requiring ICANN and the contracted parties to consider the interests of others, such as rights holders and law enforcement agencies.

[13] EDPB Letter to ICANN of 5 July 2018 (accessible here), and WP29 Letter to Göran Marby (accessible here) cautioning ICANN not conflate its own purposes with the interests of third parties.
[14] ICO guidance on the Accuracy Principle mentions: "So if you are using the data to make decisions that may significantly affect the individual concerned *or others*, you need to put more effort into ensuring accuracy". (emphasis added).

Question 2 - WHOIS ACCURACY

The memo provides, in ¶15, that GDPR's Accuracy Principle "requires controllers to take 'reasonable steps' to ensure that personal data is accurate and up to date." The memo also cites the United Kingdom Information Commissioner Office's guidance:

> The more important it is that the personal data is accurate, the greater the effort you should put into ensuring its accuracy. So if you are using the data to make decisions that may significantly affect the individual concerned ***or others***, you need to put more effort into ensuring accuracy. [emphasis added]. Memo at ¶7.

Finally, the memo provides:

a. controllers collect registration data in part to ensure the security, stability and resiliency of the Domain Name System in accordance with ICANN's mission through the enabling of lawful access for legitimate third-party interests [ICANN Purpose, Final Report EPDP at p. 21][15] and
b. the current Registrar Accreditation Agreement (RAA) requires registrars to take certain steps to ensure the accuracy of data provided by registered domain name holder (registrants).

In light of these conclusions and observations, in addition to the requirements set forth in the current Registrar Accreditation Agreement:

2.a What additional reasonable steps should ICANN and/or contracted parties take to ensure the accuracy of the data submitted with regard to the purposes for which they are processed?

2.b What additional reasonable steps should [ICANN and/or contracted parties] take to ensure the overall appropriate levels of data accuracy? In particular, would it be advisable for ICANN and/or contracted parties to implement the methods identified[16] in Bird and Bird's January 25, 2019 memo on liability related to a registrant's self-identification as a natural or non-natural person in order to ensure the overall appropriate levels of data accuracy?

2.c If statistics indicate that overall levels of data accuracy fall below a reasonable threshold (to be determined), would that demonstrate that the data controller's methods to ensure data accuracy are not reasonable?

[15] We note this reference was not included in the Accuracy memo; however, we do not think this would alter the memo.
[16] a) Confirmation emails seeking certification of the accuracy of the data submitted, b) Independent verification, c) Communicating consequences of submitting inaccurate data (under RAA, can suspend or cancel registration under certain circumstance).

Analysis

15. In this section, we examine the concept of reasonableness in respect of the Accuracy Principle (paras 14-22), we provide examples of accuracy-related measures (para 24) and we examine the use of statistics in the assessment of accuracy levels (paras 25 - 26). For the sake of clarity, we have considered that this second set of questions relates to how the Accuracy Principle applies to registration data in general and is not limited to the specific point of registrants' self-identification.

16. As set out in previous advice we have provided, although the Accuracy Principle is neither new nor specific to GDPR (or earlier EU data protection legislation), there is little case law on its precise meaning[17]. Existing case law seems to focus on the right to rectification (which is linked to but is narrower than the Accuracy Principle) and the actions (or inactivity) of controllers *after* data subjects have flagged the inaccuracy in their data and have requested its rectification; we have not found case law at EU level which examines the measures that a controller is expected or required to take in order to ensure that it collects accurate personal data in the first place.

17. Guidance from European supervisory authorities is also limited. Among the most comprehensive available guidance notes on the Accuracy Principle is the guidance provided by the UK ICO[18], which we have examined in our previous advice. In line with the wording used in the GDPR, the ICO advises that controllers need to take all reasonable steps to ensure that the personal data they hold is not incorrect or misleading as to any matter of fact. The Irish Data Protection Commissioner ("DPC") takes the same view, stating that: "*In general, the reasonable steps [...] will depend on the circumstances and in particular on the nature of the personal data and of the processing*".

18. Literature suggests that the reference to "reasonable" probably implies that it is legitimate for controllers to take into account cost and resource factors when deciding upon measures to erase or rectify data[19]. Also, that the relevant criterion to consider in respect of the Accuracy Principle will be that of a normally prudent and diligent controller[20].

19. The GDPR is not prescriptive in mandating the types of measures a controller must take to comply with the Accuracy Principle and the concept of "reasonableness" is not defined in the GDPR. This gives flexibility to ICANN and/or contracted parties to implement the measures they consider most appropriate considering the circumstances so as to sufficiently protect personal data. This approach appears to

[17] For example, in the Nowak case (C-434/16), the Court considered that "*the assessment of whether personal data is accurate and complete must be made in the light of the purpose for which that data was collected*".
[18] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/ , last accessed 31 March 2020.
[19] *Bygrave*, Data Privacy Law, An International Perspective, p. 164. The text refers to the predecessor of the GDPR, the Data Protection Directive (Directive 95/46/EC); however, the two legal texts use the same wording, hence these comments are also relevant in the GDPR context.
[20] *Boulanger, Terwangne, Léonard, Louveaux, Moreau, Poullet*, La protection des données à caractère personnel en droit communautaire, available here.

be in line with the risk-based approach promoted in the GDPR. This risk-based approach does not discharge controllers from their GDPR obligations; rather, it is based on the view that GDPR obligations should be scalable to the processing concerned and that riskier processing would entail strengthened obligations. In this respect, the Article 29 Working Party ("WP29") has clarified that fundamental principles applicable to the controllers (including the Accuracy Principle) should remain the same, whatever the processing and the risks for the data subjects. However, WP29 recognises that "*due regard to the nature and scope of processing have always been an integral part of the application of those principles, so that they are inherently scalable*"[21]. In line with the above, Article 24 GDPR imposes the obligation on controllers to implement appropriate technical and organizational measures to ensure and to be able to demonstrate their processing is carried out in accordance with the GDPR, "*taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons*".

20. In addition to these considerations, the point examined under para 9 in Question1 above should be taken into account when assessing which data accuracy measures will be reasonable, as well as the points discussed in the Legal vs Natural and the Accuracy memos. As already discussed, controllers would need to ensure that appropriate and reasonable measures are implemented at 3 stages:

    a. At the point of data collection: measures to ensure the accuracy of the data provided by data subjects;
    b. Ongoing retention period: measures to verify the personal data remains accurate and where necessary up-to-date; and
    c. Following accuracy-related requests from data subjects: measures to ensure that the rights of individuals are complied with as appropriate. A high number of requests from individuals exercising their right to correction could indicate that the level of accuracy re registrant data is not appropriate.

21. As explained in the Accuracy memo (para 21), because the reasonable and appropriate level of measures may vary depending on the circumstances and the purposes of the processing, ICANN and/or the contracted parties will be best placed to evaluate whether the procedures currently in place are sufficient or if it would be reasonable to take additional measures to comply with the Accuracy Principle – and if so, to assess which measures would be more appropriate.

22. For example, the specific circumstances of registrants' self-identification and the particular consequences of inaccurate data processing in this respect (i.e. publication of personal data without the individual's consent) would possibly require different measures compared to those applied to the collection of registrant data for the purposes of allocating a registered name to a registrant. In the first case, independent verification measures that would identify mis-labelled registrants would probably be considered reasonable, whilst in the latter context a lower threshold could possibly still be considered reasonable/acceptable and

[21] Statement on the role of a risk-based approach in data protection legal frameworks, 14/EN WP 218, available here.

controllers could rely on the data subject to provide accurate information rather than carry out independent verification.

23. A list of example measures that we have drawn on the basis of ICANN's and the contracted parties' existing practices and our recommendations included in previous advice is provided below[22]. Please note the below classification does not indicate that each measure alone would be sufficient to ensure the accurate processing of personal data – it rather provides a rough estimate of the level of "effort" that controllers might be expected to take in terms of complying with the Accuracy Principle. Depending on the circumstances, a combination of measures would provide a more appropriate level of accuracy. As there is no specific regulatory guidance in this respect, the below should be regarded as a basis for discussion amongst ICAN and contracted parties, rather than a list of definitive measures.

Measure	**Level of assurance**		
	🔴 High	🟡 Medium	🟢 Low
Accuracy-related terms in contract with data subject/ source of data (e.g. contractual obligation to provide accurate data and to notify without delay in the event of change in data)			🟢
Obligations to comply with ICANN's accuracy-related policies			🟢
Periodic review of effectiveness of accuracy measures			🟢
Confirmation email of submitted data			🟢
Verification process requiring a positive action from the data subject (e.g. click on a verification link/insert code sent to the new email address/tel. number)			🟢
Regular checks to confirm data		🟡	
Use of technical tools that identify typical errors (e.g. incorrect type of email addresses, or inexistent postcodes)			🟢
Transparency: use of plain language and clear labelling of data fields			🟢
Enhanced transparency: just-in-time notices explaining the scope and consequences of processing			🟢
Clear correction procedures following individuals' requests			🟢

[22] For the purposes of this table, we have taken into account the accuracy-related measures and provisions included in the RAA, recommendations we have previously provided in the Accuracy and Legal vs. natural memos, literature, ICO's accuracy guidance and ICO's guidance on social networking and online forums (available here).

Measures to self-rectify erroneous data	
Monitoring correction requests to identify trends and potential accuracy gaps	
Establishing accuracy thresholds and monitoring compliance with same	
Independent data verification and confirmation with data subject where data obtained from another source	
Use of automated technical systems (in particular AI)	
Engagement with supervisory authorities, industry groups, consumer/privacy advocacy groups to design/ test the effectiveness of accuracy measures	

24. The use of statistics and the monitoring of the number of correction requests from data subjects are also measures that could contribute to ensuring an adequate level of accuracy. For example, monitoring trends in rectification requests could allow to identify an accuracy gap or where a measure may not be entirely effective and take steps to cover the gap or replace the measure with a more appropriate one[23].

25. We understand the data accuracy "threshold" referenced in the question above is intended to be used as an indicator of compliance with the Accuracy Principle. Assuming that ICANN and/or the contracted parties are in a position to determine such reasonable threshold, if statistics indicate that overall levels of data accuracy in relation to registrant data fall below that threshold, this would be a strong indicator that the measures in place to ensure accuracy are not appropriate and do not meet a reasonable level.

[23] The ICO's accuracy guidance advises to carefully consider any challenges to the accuracy of personal data and to keep a note of such challenges. The GDPR examines the use of statistics from a more technical perspective in the context of profiling; Recital 71 GDPR mentions: "[…] *the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised* […]".