MEMORANDUM

|  |  |
| --- | --- |
| **To:** | Internet Corporation for Assigned Names and Numbers, EPDP Team |
| **From:** | Ruth Boardman & Gabe Maldoff |
| **Date:** | 8 February 2019 |
| **Subject:** | Advice on the meaning of the accuracy principle pursuant to the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR") |

**Question Presented**

1. Some EPDP Team members cite Art. 5.1(d) of the GDPR as a requirement for the EPDP Team to examine how accuracy is currently defined in ICANN’s 2013 Registrar Accreditation Agreement (the contract with registrars) and possibly require changes. Some EPDP Team members cite the accuracy requirement in Art. 5.1(d) GDPR as support for additional accuracy related policies, such as a requirement for registrars to validate the correctness of the data as provided by the data subject or a requirement to validate when the accuracy is being challenged. Others maintain that the Art. 5.1(d) GDPR requirement is to accurately record, maintain and process the data provided by the data subject and to update that information as informed by the data subject. Is the accuracy requirement limited to correction at the request of the data subject or is it a broader requirement? Please advise on how the accuracy requirements of GDPR impact the contracted parties and ICANN.

**Legal Background**

1. Article 5(1)(d) (the "Accuracy Principle") states that personal data must 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*".
2. Despite the fact that the Accuracy Principle is a longstanding feature of data protection laws, dating back at least as far as the 1980 OECD Privacy Principles,[[1]](#footnote-1) there is little case law or guidance on its precise meaning.[[2]](#footnote-2)
3. The Accuracy Principle appears in the Council of Europe's Convention 108, which was the forerunner to European Union data protection law. The Council of Europe and the European Data Protection Supervisor jointly produced a Handbook on European Data Protection Law, which explains both Convention 108 and the GDPR. With respect to the Accuracy Principle, the Handbook concludes that in some circumstances, controllers may have a positive obligation to ensure that the personal data under their control is accurate[[3]](#footnote-3): "*A controller holding personal information shall not use that information without taking steps to ensure with reasonable certainty that the data are accurate and up to date. The obligation to ensure accuracy of data must be seen in the context of the purpose of data processing*".
4. Based on our review of guidance from supervisory authorities in the UK, Belgium, Ireland and Germany, the UK Information Commissioner’s Office ("ICO") offers the most comprehensive guidance on this requirement[[4]](#footnote-4). In its guidance, the ICO suggests that complying with the Accuracy Principle requires an assessment of three separate questions:
	1. What is the obligation to verify that personal data collected by the controller is accurate at the time of collection?
	2. What is the controller's on-going responsibility to ensure that personal data remains accurate and up-to-date?
	3. What must a controller do upon receiving a request from a data subject relating to the accuracy of personal data?
5. ***Ensuring the accuracy of personal data provided by the data subject***
6. At least under some circumstances, there is a positive obligation on the controller to ensure that the data is accurate. However, the existence of such a positive obligation is contextual – it depends on the significance of the consequences for data subjects of processing inaccurate data and the effort that would be required to verify accuracy.
7. 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*".
8. The GDPR is not prescriptive in mandating the types of measures a party must put in place to meet this burden. The ICO guidance explains that "*[w]hat is a ‘reasonable step’ will depend on the circumstances and, in particular, the nature of the personal data and what you will use it for*". As a general rule, the ICO guidance says it is usually reasonable to assume information given by the data subject is accurate, "*unless inaccurate information could have serious consequences, or if common sense suggests there may be a mistake*".
9. A controller "*may have to get independent confirmation*" where the impact is particularly significant. For example, where an employer engages employees needing essential qualifications to be able to fulfil the job description, it would be reasonable to independently verify an applicant's credentials. By contrast, where an individual completes a lifestyle survey, which will be used for research and direct marketing, with information about interests, there is no obligation on the organisation to verify the accuracy of the information.
10. ***Verifying that personal data remains accurate***
11. In terms of the requirement to ensure that personal data remains up to date, the same analysis applies. The ICO guidance states that "*it is reasonable to rely on the individual to tell you when their personal data has changed*". However, in some cases, "[i]*t may be sensible to periodically ask individuals to update their own details, but you do not need to take extreme measures to ensure your records are up to date, unless there is a corresponding privacy risk which justifies this*"*.*
12. For example, if an organisation keeps contact details as part of its marketing lists, "*[i]t does not have to use data matching or tracing services to ensure its records are up to date – and it may actually be difficult to show that the processing involved in data matching or tracing for these purposes is fair, lawful and transparent*".
13. ***Responding to correction requests***
14. Individuals have a right to correct inaccurate data. The ICO guidance on the right to rectification[[5]](#footnote-5) applies similar principles as above apply to the determination of whether data is, in fact, inaccurate: if an individual requests the correction of their personal data, the controller must take reasonable steps to verify the accuracy, in light of the circumstances and the risks to the individual caused by the inaccuracy. While not related to this specific question, the ICO also notes that special procedures may be required when the fact that the data was mistaken is relevant. In those cases, the ICO recommends retaining the mistaken data as well as the updated information.
15. Controllers must respond to correction requests "*without undue delay and in any event within one month*". However, the time limit may be extended a further two months depending on the complexity and number of requests. If time is needed to verify the accuracy of the data, data subjects are permitted to request the restriction of it (i.e. that the data not be used for other purposes until its accuracy is verified).

**ICANN Registrar Accreditation Agreement**

1. ICANN's Registrar Accreditation Agreement (the "**Agreement**") contains provisions that are relevant to the Accuracy Principle. While these provisions may be intended, at least in part, for authentication reasons rather than solely to verify accuracy, they are nonetheless relevant for the application of the Accuracy Principle.

|  |  |
| --- | --- |
| **Element of Accuracy Principle** | **Relevant Agreement Provisions** |
| 1. *Verification of data provided*
 | * Registrars must include the following in their terms with Registered Name Holders ("**RNHs**"):
	+ The RNH must provide "*accurate and reliable contact details*" *and correct and update them within seven (7) days of any change during the term…*"[[6]](#footnote-6); and
	+ The wilful provision of inaccurate or unreliable information, or a wilful failure to update information or respond to inquiries from the Registrar concerning accuracy is a material breach and cause for the suspension and/or cancellation of the registration.[[7]](#footnote-7)
* At the time of registration, upon a transfer of the sponsorship of a registration to the Registrar, or upon any change to the contact information in the registration, the Registrar must:
	+ Verify the contact details of the RNH in one of several ways that each requires an affirmative response from the RNH and proof, using a unique code. The registration must be suspended if the RNH does not respond, unless the Registrar manually verifies the RNH's contact details.[[8]](#footnote-8)
	+ Verify the contact details of the Account Holder (if different from the RNH) in the same way; however, the Registrar is not required to suspend the registration if the contact details cannot be verified.[[9]](#footnote-9)
	+ There are exceptions if the Registrar has already completed a verification and there is no reason to believe the contact information is inaccurate.[[10]](#footnote-10)
* Registrars must comply with any Consensus Policy requiring "*reasonable and commercially practicable*" verification of information at the time of registration.[[11]](#footnote-11)
 |
| 1. *Verification of stored data*
 | * Registrars must include in their terms with Registered Name Holders ("**RNHs**") that:
	+ The RNH must provide "*correct and update [contact details] within seven (7) days of any change during the term…*"[[12]](#footnote-12); and
	+ The wilful failure to update information or respond to inquiries from the Registrar concerning accuracy is a material breach and cause for the suspension and/or cancellation of the registration.[[13]](#footnote-13)
* Registrars must comply with any Consensus Policy requiring "*reasonable and commercially practicable*" periodic re-verification of information.[[14]](#footnote-14)
	+ The Whois Data Reminder Policy[[15]](#footnote-15) requires Registrars to send an annual reminder to registrants. The reminder includes details of the contact information for the registrant, administrative contact and technical contact. The registrant is offered to opportunity to correct errors, but is not required to respond.
* If a Registrar has any information suggesting that contact information is incorrect (e.g. because a Whois Data Reminder email bounces back), the Registrar must verify the contact details as it would for a new registration.[[16]](#footnote-16)
 |
| 1. *Data subject requests*
 | * "*Registrar shall, upon notification by any person of an inaccuracy in the contact information associated with a Registered Name sponsored by Registrar, take reasonable steps to investigate that claimed inaccuracy. In the event Registrar learns of inaccurate contact information associated with a Registered Name it sponsors, it shall take reasonable steps to correct that inaccuracy*".[[17]](#footnote-17)
 |

**Analysis**

1. The Accuracy Principle requires controllers to take "reasonable steps" to ensure that personal data is accurate and up-to-date. In some instances, it is reasonable for a controller to rely on the person submitting the data to provide data that is accurate. In other instances, the GDPR requires controllers to take affirmative steps to ensure that the data submitted is indeed accurate. What steps are appropriate will depend on the circumstances and the nature of the risks presented to data subjects.

1. The Agreement sets out procedures by which Registrar's must actively verify data they receive and periodically confirm that it remains up to date. Registrars are also tasked with reasonably responding to requests from data subjects. As the GDPR requirement turns on what is reasonable under the circumstances, only ICANN and the relevant parties can confirm that these procedures are indeed sufficient. However, the procedures required by the Agreement certainly seek to address accuracy, as per the GDPR's Accuracy Principle.
2. The Agreement's procedures require Registrars to take affirmative steps to confirm that data provided by registrants is accurate. The Registrar is required to contact the registrant via the contact details provided and to suspend a registration if the registrant does not confirm in an appropriate manner.
3. Likewise, the Agreement – and the corresponding Whois Data Reminder Policy – requires the Registrar to confirm registration details with the registrant on an annual basis. This addresses a potential concern that registration data may become out of date.
4. 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.[[18]](#footnote-18)
5. The Agreement is less specific on the procedure required for responding to data subject requests. Instead, Registrars are subject to a requirement to take reasonable steps to investigate the request and correct any inaccuracy. Nonetheless, the lack of specificity does not raise obvious concerns: registrars will be well-placed to determine how to respond to such requests and will be subject to independent obligations under GDPR to respond effectively.
6. 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 *in*sufficient, we see no clear requirement to review them.
1. The OECD Principles contained a "*Data Quality Principle*", which incorporated a similar concept of accuracy: "*Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date*". [↑](#footnote-ref-1)
2. We were unable to find any case law in the UK, Belgium or Germany directly addressing the meaning of accuracy as relevant to this query within the time we had. Nor could we find any guidance in Ireland. We would be happy to check in additional Member States if this would be helpful. [↑](#footnote-ref-2)
3. https://www.echr.coe.int/Documents/Handbook\_data\_protection\_02ENG.pdf. [↑](#footnote-ref-3)
4. ICO Guide to the GDPR, Principle (d): Accuracy, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/. [↑](#footnote-ref-4)
5. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/. [↑](#footnote-ref-5)
6. Section 3.7.7.1. [↑](#footnote-ref-6)
7. Section 3.7.7.2. [↑](#footnote-ref-7)
8. WHOIS Accuracy Program Specification, para. 1. [↑](#footnote-ref-8)
9. WHOIS Accuracy Program Specification, para. 1. [↑](#footnote-ref-9)
10. WHOIS Accuracy Program Specification, para. 3. [↑](#footnote-ref-10)
11. Section 3.7.8. [↑](#footnote-ref-11)
12. Section 3.7.7.1. [↑](#footnote-ref-12)
13. Section 3.7.7.2. [↑](#footnote-ref-13)
14. Section 3.7.8. [↑](#footnote-ref-14)
15. https://www.icann.org/resources/pages/registrars/consensus-policies/wdrp-en. [↑](#footnote-ref-15)
16. WHOIS Accuracy Program Specification, para. 4. [↑](#footnote-ref-16)
17. Section 3.7.8. [↑](#footnote-ref-17)
18. In previous advice, we suggested that Registrars could contact technical and administrative contacts as a way of ensuring that transparency requirements are met. If ICANN will adopt this suggestion, then Registrars could also verify accuracy at the same time. [↑](#footnote-ref-18)