MEMORANDUM

|  |  |
| --- | --- |
| **To:** | Internet Corporation for Assigned Names and Numbers, EPDP Team |
| **From:** | Ruth Boardman & Gabe Maldoff |
| **Date:** | 8 March 2019 |
| **Subject:** | Advice on the legal basis for transferring Thick WHOIS |

1. **Question presented**
	1. Is there a legal basis under GDPR to justify a transfer of data elements from registrars to registries[[1]](#footnote-1) even though the processing and transfer of data may be to enable processing for the benefit of 3rd parties pursuant to ICANN's thick Whois policy?
2. **Factual background**
	1. Prior to 1 February 2019,[[2]](#footnote-2) generic top-level domain ("**gTLD**")registries and registrars could satisfy their Whois obligations using one of two common service models.
		1. Under the "thin Whois" model, registries stored only the information associated with the domain name. This included data that identifies the sponsoring registrar, the status of the registration, creation and expiration dates for each registration, name server data, the last time the record was updated, and the URL for the registrar's Whois service. Registrars, by contrast, managed the full set of Whois data, including data associated with the registrant.
		2. Under the "thick Whois" model, the full set of WHOIS data was managed by both the registry and the registrar.
	2. On 22 September 2011, the Generic Names Supporting Organization ("**GNSO**") requested an Issue Report on "thick Whois". The resulting Final Report on the Thick Whois Policy Development Process (the "**Thick Whois Report**"), issued on 21 October 2013, recommended that "*the provision of thick Whois services … should become a requirement for all gTLD registries, both existing and future*".
	3. Following adoption by the GNSO of the Thick Whois Report, ICANN's Board resolved to implement a thick Whois policy,[[3]](#footnote-3) the final element of which came into effect on 1 February 2019.
	4. According to the Thick Whois Report, the policy was motivated by security, stability and reliability concerns, among others:
		1. First, the thick Whois model is helpful for maintaining the stability of directories in the event that a registrar experiences a technical failure or goes out of business. Centralising the storage of the full Whois data set in registries (while at the same time maintaining copies held by registrars) reduces the likelihood of service disruptions.
		2. Second, the thick Whois model facilitates the transfer of domain registrations from one registrar to another. By ensuring that registries maintain a full set of Whois data, it is easier for a receiving registrar to obtain the required data in a standard format.
		3. Third, the thick Whois model reduces the variability of display formats and improves data quality, by better positioning registries to undertake checks that data remains up to date and accurate.
	5. In the Thick Whois Report, the Working Group considered the effects of the thick Whois model on data protection and privacy. The Report concluded that, although the thick Whois model potentially introduced greater security concerns because the full data set would be stored by a larger number of actors, such effects were negligible given that the full Whois data set was, at that time, made publicly available in both the thick and thin models.
	6. The Final Report pre-dates ICANN's Temporary Specification and the development of a Consensus Policy to mask the display of full Whois data in response to the coming into force of the GDPR (together, the "**Temp Spec**"). The Temp Spec introduced a process by which registries and registrars may only disclose certain Whois data pursuant to requests that align with certain pre-defined purposes ("**Authorised purposes**").
	7. Therefore, in light of the Temp Spec, it is appropriate to consider whether it remains the case that the thick Whois model "*does not raise data protection issues that are specific to thin vs. thick Whois*", as was found in the Thick Whois Report, and whether it accords with the GDPR.
3. **Analysis**
	1. Registrars can justify sharing *some* Whois data with registries on the basis of Article 6(1)(b) of the GDPR, since some sharing will be "*necessary for the performance of a contract to which the data subject is party*" – i.e. to provide the registration service to the data subject. However, not all data shared with registries will be considered necessary.[[4]](#footnote-4) As evidenced by the fact that the system functioned on a thin Whois model at one time, registries do not need access to the full thick Whois data set in order for the service to be provided to registrants.
	2. In the absence of European Union or Member State legislation that either mandates the sharing of thick Whois data (Article 6(1)(c)) or sets out a clear public interest for sharing the full data set (Article 6(1)(e)), the only available legal basis for sharing more personal data than required to perform the contract is Article 6(1)(f) of the GDPR ("**legitimate interests**").[[5]](#footnote-5)
	3. In order to satisfy the legitimate interests test, the Court of Justice of the European Union ("**CJEU**") held, in *Valsts policijas Rigas regiona parvaldes Kartibas policijas parvalde v* Rigas *pašvaldibas SIA ‘Rigas satiksme’* (the "***Rigas***" case), that there must be (a) an identified legitimate interest, (b) the processing must be "*necessary*" to pursue that interest, and (c) the rights and interests of the data subject must not outweigh the legitimate interest pursued by the controller.

***The purposes motivating the thick Whois policy are legitimate and the processing is necessary for these purposes***

* 1. The GDPR Recitals provide examples of activities that could be considered legitimate interests, where not outweighed by the rights and interests of data subjects. For example, Recital 48 states, "C*ontrollers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data*".
	2. This example makes clear that the sharing of personal data among affiliated entities for internal administrative purposes may be considered a legitimate interest. The Recitals also cite security, including preventing denial of service attacks, as a legitimate interest for processing personal data.
	3. The thick Whois policy is animated by a desire to improve stability, security and reliability of the gTLD registration system. These will be considered legitimate interests under the GDPR.
	4. The benefits of this policy accrue not only to registries and registrars, but also to third-parties that rely on being able to access Whois data, such as rights holders and law enforcement.
	5. The fact that the policy serves the interests of third-parties does not undermine the legitimate interests test. Article 6(1)(f) states that personal data may be processed where it is "*necessary for the purposes of the legitimate interests pursued by the controller or by a third party …*". The CJEU recognised this in the Rigas case, when it held that "*the interest of a third party in obtaining the personal information of a person who damaged their property in order to sue that person for damages can be qualified as a legitimate interest*".
	6. Moreover, in Opinion 06/2014 *on the notion of legitimate interests of the controller*, the Article 29 Working Party ("**WP29**") found that, "*[i]n general, the fact that a controller acts not only in its own legitimate (e.g. business) interest, but also in the interests of the wider community, can give more 'weight' to that interest*".
	7. It is implicit in the Thick Whois Report that the previous system posed certain risks to the security, stability and reliability of gTLD registrations and that there was no less intrusive way of addressing these concerns. Therefore, the shift to a thick Whois policy was considered to be necessary.

***The impacts of thick Whois on data subjects***

* 1. The Thick Whois Report concluded that the impact on individuals of changing to a thick Whois model was negligible. However, that conclusion was in part dependent on the fact that registrars made full thick Whois data publicly available in any event – in those circumstances, no additional risk would arise from sharing the data with registries. Under the Temp Spec, which mandates that thick Whois data is no longer publicly available, this operative fact has changed. Nonetheless, we conclude that the impact of sharing thick Whois data with registries remains negligible.
	2. In sum, the thick Whois model could affect individuals in two ways: (a) ease of access to personal data and (b) security. The second was addressed in the Thick Whois Report; the first was not.

***The impact on ease of access to personal data***

* 1. The thick Whois model eliminates a step that stakeholders might need to undertake in order to access the full Whois data set. Whereas under the thin Whois model, a stakeholder might need to first consult the registry to identify the relevant registrar before approaching the registrar to access the data, under the thick Whois model, the stakeholder would be able to obtain the full data set from the registry directly (provided the stakeholder can demonstrate an Authorised Purpose).
	2. European Union law recognises that the relative ease of accessing personal data, or so-called "practical obscurity", is an important consideration in protecting personal data. For example, in *Google Spain SL and Google Inc. v. AEDP and Mario Costeja González* ("***Google Spain***"), the CJEU required Google to de-list search results to newspaper articles that were inadequate, irrelevant or excessive, but it did not require the underlying articles to be taken down. Even though the articles would continue to exist on the newspaper's website, this did not guarantee Google a legitimate interest in processing the personal data contained within the articles (i.e. by crawling and indexing search results).
	3. A similar principle can be drawn from *Camera di Commercio, Industria, Aritigianato e Agricoltura di Lecce v. Salvatore Manni* ("***Manni***"), where the CJEU resisted the application of the right to be forgotten to the Lecce Chamber of Commerce. In support of a legitimate interest in the publication of bankruptcy and insolvency data, the CJEU noted "*the need to protect the interests of third parties in relation to joint-stock companies and limited liability companies and to ensure legal certainty, fair trading and thus the proper functioning of the internal market*". Thus, the CJEU's analysis took into account the audience most likely to access the data. Both *Google Spain* and *Manni* address data that is publicly published, but in the *Manni* case, the Lecce Chamber of Commerce's legitimate interest was supported by the fact that the data was more likely to be accessed only by those with legitimate business needs.
	4. While these cases demonstrate that the difficulty of accessing personal data (i.e. conducting a Google search vs. consulting a website directly) can affect the balance of interests between the parties, in our view, the additional protections afforded by a thin Whois model as opposed to a thick Whois model are too marginal to affect the legitimate interests test in this case.
	5. The Temp Spec ensures that personal data is not disseminated more widely than ICANN and the relevant parties deem to be appropriate. The difference between a thick and thin Whois policy would mean that stakeholders would need to take only one minor additional step (i.e. checking a registry to identify the relevant registrar) in order to access restricted data. The more significant restriction is the need to demonstrate an Authorised Purpose, which would be a requirement regardless of the volume of Whois data shared between the relevant parties.
	6. Against this marginal change in the level of access to personal data, ICANN and the relevant parties articulated clear benefits to implementing the thick Whois policy for security, stability and reliability purposes, such as to ensure that registration data can be transferred to another registrar more easily in case of a technical outage or bankruptcy. In addition, the Thick Whois Report noted that this model would improve the accuracy of records by putting registries in a position to analyse and improve data quality.

***The impact on security***

* 1. The Thick Whois Report noted that the thick Whois model would result in a greater number of parties holding a copy of the data (i.e. the registry, registrar and their escrow agents will have access, as opposed to just the registrar and its escrow agent). The Report expressed a concern that increasing the number of copies of the database could increase the likelihood of a breach, but ultimately concluded that such concern was minimal given that Whois data was as a rule made publicly available at the time.
	2. Under the Temp Spec, this concern is more significant because the data is no longer publicly accessible without an Authorised Purpose. However, this additional risk does not, in our view, need to affect the legitimate interests balancing test. Article 32 of the GDPR requires controllers and processors to implement appropriate security to protect personal data, taking into account the risks to data subjects, the state of the art and the costs of implementation. By centralising thick Whois data in the registries, the security risks faced by registries increase. However, provided these are addressed by commensurate measures, as registries are required to do under Article 32, the balance of interests will not be affected.
1. Registries and registrars are controllers; therefore, they each need a legal basis for processing personal data. Processors do not need to have a legal basis because they act under the instructions of the controller. [↑](#footnote-ref-1)
2. https://www.icann.org/news/announcement-2-2017-02-01-en. [↑](#footnote-ref-2)
3. https://gnso.icann.org/en/group-activities/active/thick-whois. [↑](#footnote-ref-3)
4. *See* our Advice on Interpretation of Article 6(1)(b) of the General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR"), dated 23 January 2019, in which we concluded that "*a registrar cannot make processing in order to prevent DNS abuse contractually necessary simply by including a reference to this in its contract with the registered name holder*". [↑](#footnote-ref-4)
5. Consent, pursuant to Article 6(1)(a), is also not a viable option because, under the thick Whois policy, the sharing of Whois data between registrars and registries is mandatory. [↑](#footnote-ref-5)