MEMORANDUM

|  |  |
| --- | --- |
| **To:** | Internet Corporation for Assigned Names and Numbers, EPDP Team |
| **From:** | Ruth Boardman & Phil Bradley-Schmieg |
| **Date:** | 27 April 2021 |
| **Subject:** | March 2021 question re. EU and third-party recognition of registration data publication interests |
|  |  |

Background

1. The EDPB, in a July 2018 letter to Göran Marby (the “EDPB July 2018 Letter”),[[1]](#footnote-1) stated that:

“personal data identifying individual employees (or third parties) acting on behalf of the registrant should not be made publicly available by default in the context of WHOIS”.

This has prompted several GDPR-related questions, most recently in our memorandum dated 6 April 2021 (the “**VSC and Consent Options Memorandum**”), which discussed two questions (“**Question 1 and Question 2”**) discussing different approaches (and resulting risks) in respect of (i) consent-conditional publication of registration data; and (ii) publication of registration data if it relates (only) to a legal person (e.g. a company), rather than being personal data (and how this can be verified) – i.e. Verified Self-Characterisation, “VSC”.

You have also asked, in the question presented below, whether certain provisions in EU legislation, and/or the practices of two third parties (EURid, and the RIPE-NCC), create helpful precedent in this area. This memorandum addresses that third question.

|  |
| --- |
| **Question presented**: Commission Regulation (EC) No 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration (‘.eu Regulation’) sets out the public policy rules concerning the implementation and functions of the .eu Top Level Domain (TLD) and public policy principles on registration of domain names in the .eu TLD. Article 16 of the .eu Regulation is entitled ‘Whois database’ and provides: *‘The purpose of the WHOIS database shall be to provide reasonably accurate and up to date information about the technical and administrative points of contact administering the domain names under the .eu TLD.**The WHOIS database shall contain information about the holder of a domain name that is relevant and not excessive in relation to the purpose of the database. In as far as the information is not strictly necessary in relation to the purpose of the database, and if the domain name holder is a natural person, the information that is to be made publicly available shall be subject to the unambiguous consent of the domain name holder. The deliberate submission of inaccurate information, shall constitute grounds for considering the domain name registration to have been in breach of the terms of registration.’* As from 13 October 2022, the .eu Regulation will be repealed by Regulation 2019/517, which provides under Article 12, entitled WHOIS database: ‘*1. The Registry shall set up and manage, with due diligence, a WHOIS database facility for the purpose of ensuring the security, stability and resilience of the .eu TLD by providing accurate and up-to-date registration information about the domain names under the .eu TLD.**2. The WHOIS database shall contain relevant information about the points of contact administering the domain names under the .eu TLD and the holders of the domain names. The information on the WHOIS database shall not be excessive in relation to the purpose of the database. The Registry shall comply with Regulation (EU) 2016/679 of the European Parliament and of the Council.*’ The Whois database is currently administered by EURid, a non-profit designated by the European Commission to manage the .eu registry. In its Whois database, EURid publishes the email addresses of domain name registrants in the .eu TLD (both natural persons and legal entities). EURid distinguishes between natural persons and legal entities by publishing the postal address information of legal entities, whereas this information is not published for natural persons.  Through Article 16 of the .eu Regulation, EURid is able to rely on GDPR Article 6(1)(e), which provides a legal basis for processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.  While we understand that this Article 16 public interest basis is not available outside the .eu domain, the existence of this lawful basis for EURid’s processing could be interpreted to suggest that the EU legislature recognized that disclosure of the Registrant data serves a legitimate interest in stability, security, and resilience.  Further, in carrying out its mandate under Article 16, EURid has determined that publication of the Registrant’s email “is not excessive in relation to the purpose of the database.”   Similarly, while RIPE-NCC relies on consent to publish personal information about tech/admin contacts, it publishes personal information about resource holders on the grounds that “facilitating coordination between network operators is the one purpose that justifies the publication of personal data in the RIPE-NCC database and that it is clear that the processing of the personal data referring to a resource holder is necessary for the performance of the registry function, which is carried out in the legitimate interest of the RIPE community and the smooth operation of the Internet globally (and is therefore in accordance with article 6.1.f of the GDPR).” We understand that the public interest basis supplied by Article 16 is not available to Contracted Parties outside of the .eu top level domain.  Based on your experience and applicable precedent to what extent if any do:(i) the existence of Article 16 of the EU Regulation; (ii) EURid’s decision to publish Registrant email addresses consistent with Article 16, (iii) RIPE-NCC’s decision to publish the email addresses of resource holders; and (iv) draft language regarding access to registration data in the recently proposed NIS2 Directive create precedent that would reduce Contracted Party  risk in connection with publication of a legal person Registrant’s email address, even if it contained personal information? Do these facts affect your answers to Questions [1-2]? If it does not affect your answers, please explain why. |

We believe that overall, the cited documents do not affect our answers to Questions 1 and 2 in the VSC and Consent Options Memorandum. More specifically, we believe the cited documents have limited impact on Contracted Party risk in connection with publication of a legal person Registrant’s email address, even if it contained personal data. Our view is based on the reasons set out below.

*Regulation (EU) 2019/517, replacing Commission Regulation (EC) No 874/2004 (the “New .EU Regulation”)*

When Regulation (EU) 2019/517 (the “New .EU Regulation”) replaces Commission Regulation (EC) No 874/2004 (the “Old .EU Regulation”), it will delete a provision of the Old .EU Regulation that allowed for the “not strictly necessary” publication of personal data in Registration Data (if the data subject expressly consented to this). The relevant provisions are quoted in the question presented.

The New .EU Regulation does not expressly say that a consent-driven approach has proven to be impractical or non-compliant; it simply offers no comment on such an approach. In fact, the New .EU Regulation now does not make any comment specifically about the publication of personal data, whether “strictly necessary” or otherwise. It limits itself to requiring that the data processing complies with the GDPR (if applicable), without saying how. In particular, Recital 22 of Regulation (EU) 2019/517 specifically requires the .eu Registry to choose an implementation of the WHOIS database and related systems that complies with “personal data protection by design and data protection by default”, “necessity” and “proportionality”.

The most direct reference to distribution of the registration data, if it is personal data, can be found in Recital 21. This speaks only about data sharing with/access *by law enforcement agencies*, acting pursuant to “[EU] or national law” – *not* the public at large, *nor* interested parties such as IP rightsholders:[[2]](#footnote-2)

“21. The Registry should support law enforcement agencies in the fight against crime, by implementing technical and organisational measures aimed at enabling competent authorities to have access to the data in the Registry for purposes of the prevention, detection, investigation and prosecution of crimes, as provided for by Union or national law*.*”

In essence, the New .EU Regulation strikes a mostly neutral and inconclusive position here. It generally defers to GDPR requirements, and *specifically* calls out a need to respect proportionality and privacy by default. The fact that it discusses legitimate access by *specific* stakeholder groups, does not necessarily exclude a system in which some personal data is made public, e.g. with a data subject’s consent. Nevertheless, the New .EU Regulation has dropped wording (found in its predecessor) that explicitly accepted an approach founded (in part) on consent; it is possible that a supervisory authority or court might seek to draw an adverse inference from this.

*EURid’s reliance on the GDPR “public task” legal basis*

The question posed suggests that EURid relies on Article 16 of the Old .EU Regulation to assert that its (partial) publication of registrants’ personal data is permitted by GDPR Article 6(1)(e).

GDPR Article 6(1)(e) permits processing that is necessary for the performance of a task carried out either in the public interest or in the exercise of official authority vested in the controller. These must be laid down in EU or EU Member State law.

If the question’s suggestion is correct,[[3]](#footnote-3) then EURid is implicitly asserting that such publication is “strictly necessary in relation to the purpose of the database”. If that were not the case, then EURid would be operating in breach of Article 16 of the Old .EU Regulation, since this states that “In as far as the information is not strictly necessary in relation to the purpose of the database, and if the domain name holder is a natural person, the information that is to be made publicly available shall be subject to the unambiguous consent of the domain name holder.” Based on the question posed, we understand that EURid does not obtain such consent.

On the one hand, this presumed position indicates that at least one Registry (EURid) upholds the importance (“strict necessity”) of publishing (some) data in WHOIS, even if it is personal data, and without consent or measures such as VSC (provided, at least, that some of the personal data is redacted, as per EURid’s policy on the matter).[[4]](#footnote-4)

However, the view held by EURid is not necessarily reflective of the views of the courts or supervisory authorities that enforce the GDPR – and is not binding on them. It is the view of one Registry, among others. The fact that this particular Registry’s policies are also subject to European Commission supervision[[5]](#footnote-5) is of similarly limited precedential value; even if – hypothetically – this is a question that has been discussed between EURid and the European Commission, the latter does not enforce the GDPR, nor speak for those who do.

The question presented further states that “EURid distinguishes between natural persons and legal entities by publishing the postal address information of legal entities, whereas this information is not published for natural persons”. EURid’s current [Registration Policy (v.11)](https://eurid.eu/d/7568041/Registration_Policy_EN.pdf) explains that “Where no undertaking or organisation name is specified, the individual requesting registration of the Domain Name will be considered the Registrant; if the name of the undertaking or organisation is specified, then the undertaking or organisation is considered the Registrant”.

This may mean that an assumption is made that postal details provided by an organisation (a legal person registrant) *do not* contain personal data; or simply that if it does so, this is strictly necessary and/or lower risk for individuals. EURid – as the controller of much of the data in question – will be better placed than we are to determine whether that assumption holds true in practice.

Even if that assumption hypothetically holds true for EURid and the postal addresses it publishes as part of legal persons’ .eu registration data, we note that in light of the EDPB’s comments to ICANN,[[6]](#footnote-6) it may be inadvisable to extrapolate from this to other contact information (e.g. email addresses, which might refer specifically to one readily-identifiable individual within the organisation).

Based on those observations, plus an appreciation that EURid operates within a somewhat unique legislative framework giving it the option to rely on something other than consent or legitimate interests – unlike other Contracted Parties – it is therefore difficult to draw any general conclusions from EURid’s approach.

*The RIPE-NCC’s decision to publish the email addresses of resource holders*

The question posed quotes from a blog post from 2018 authored by the RIPE-NCC’s Head of Legal, entitled “[How We're Implementing the GDPR: Legal Grounds for Lawful Personal Data Processing and the RIPE Database](https://labs.ripe.net/Members/Athina/gdpr-legal-grounds-for-lawful-personal-data-processing-and-the-ripe-database)”.

In that blog post, as the question posed correctly states, the RIPE-NCC states that it relies on legitimate interests (the GDPR Art. 6(1)(f) legal basis) for publishing personal data – primarily contact details – to assist with the proper functioning of an important Internet system.

It should be noted, however, that the blog post also states:

*“*However, when the resource holder appoints another individual to perform this role [i.e., as a contact point], they must obtain the consent of the person(s) whose personal data will be inserted in the RIPE Database before their data is inserted (in accordance with Article 6.1.a of the GDPR).*”*

In other words, it appears to us that when the resource-holder itself is a legal person, (i) the RIPE-NCC views legitimate interests as an appropriate legal basis in first party settings (i.e. when the person completing/updating a registration provides their own contact details, and are therefore the relevant data subject), but (ii) the RIPE-NCC had (at least, in 2018) instead preferred to do this only with a data subject’s consent in third party settings (e.g. when the contact details are those of a colleague of the person completing/updating the registration).

This distinction might be due to fears that it would be harder to assert that the third party’s own interests are sufficiently aligned with those of the resource-holder and/or the RIPE-NCC (and related stakeholders); and/or fears that there are greater risks for third party data subjects (for instance because it is more difficult to provide a GDPR privacy notice to them, so they may be less aware of their rights). Such concerns may therefore have driven the RIPE-NCC to instead prefer to rely on consent for those “third party” situations.

While the RIPE-NCC must seek its own legal advice on the matter, our view so far as the ICANN-EPDP is concerned is that such a distinction may not be legally required. GDPR Article 6(1)(f) (the legitimate interests basis) does not require the data subject’s interests to be aligned with those of the controllers(s) – merely, there must be an appropriate *balance* between the interests at stake (those of the controller and/or of third parties), versus the “fundamental rights and freedoms of the data subject which require protection of personal data”. In this case, the RIPE-NCC and its own legal advisors will have the best insight into the various interests and risks, however it appears to us that:

* 1. The interests *of the controller and wider stakeholders* would seem to be broadly the same whether dealing with a first party or third party’s contact details: e.g. either set of contact details are presumably important for the proper investigation and resolution of disruptions to a key Internet system;
	2. On the risks side, first party or third party contact details could equally be abused, e.g. for unsolicited marketing; there may be other types of risk, but once again, those seem likely to be similar whether for first party or third party data subjects;
	3. As for the notice issue, the GDPR specifically accepts that there will be situations where data is not collected directly from a data subject, and notice might therefore not be provided to them (see, in particular, GDPR Article 14(5)). This therefore is not an automatic reason to dismiss the potential use of legitimate interests in third party settings; and
	4. It may be for this reason that the EDPB’s letter to ICANN, in July 2018, endorsed potential reliance on legitimate interests even for third-party data, provided that registrants are not *compelled* to provide such third party data, but can instead provide their own.[[7]](#footnote-7) We understand that this is indeed the case for the system overseen by the RIPE-NCC.

The RIPE-NCC likely feels that regulators and courts would at first glance welcome the autonomy and control offered by reliance on consent, rather than a non-consensual GDPR legal basis like legitimate interests. However, those authorities might also recognise the practical downsides of such an approach:

* 1. The RIPE-NCC’s own blog post acknowledges the doubts that sometimes surround consents obtained in employment contexts (i.e., that such consents, if requested by an employer, may not have been freely given by an employee).
	2. The RIPE-NCC also ends up relying on the first party’s representations that they have obtained a valid consent from the third party (“The RIPE NCC considers that it is the responsibility of the one who inserts the data in the RIPE Database (i.e. the maintainer) to ensure that they have obtained valid consent for the processing to take place.”). This could make it difficult, in theory, for the RIPE-NCC (as controller) to demonstrate that those consents met all GDPR requirements.
	3. Contracted Parties could face the same GDPR issues in respect of domain name registration data.

The views of the RIPE-NCC are, like those of EURid, not necessarily reflective of – and certainly not binding on – authorities tasked with GDPR enforcement.

Moreover, the legitimate interests balancing exercise to be conducted by the RIPE-NCC is different to that of ICANN and Contracted Parties; the data in question relates to different resources (IPv4, IPv6 and AS Number resources, often allocated by the RIPE-NCC – in blocks – to very large organisations; versus specific domain names sometimes being registered by specific individuals for private use).

It is therefore difficult to draw any general conclusions from the RIPE-NCC’s approach.

*Draft language regarding access to registration data in the recently proposed NIS2 Directive*

In December 2020, the European Commission published its draft for a [revised Directive on measures for a high common level of cybersecurity across the Union (“NIS2”)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823).

The Recitals of the proposed NIS2 Directive state that:

“15. Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to all providers of DNS services along the DNS resolution chain, including operators of root name servers, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers.

(…)

(59) Maintaining accurate and complete databases of domain names and registration data (so called ‘WHOIS data’) and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. Where processing includes personal data such processing shall comply with Union data protection law.

(60) The availability and timely accessibility of these data to public authorities, including competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, CERTs, (CSIRTs, and as regards the data of their clients to providers of electronic communications networks and services and providers of cybersecurity technologies and services acting on behalf of those clients, is essential to prevent and combat Domain Name System abuse, in particular to prevent, detect and respond to cybersecurity incidents. Such access should comply with Union data protection law insofar as it is related to personal data.

(61) In order to ensure the availability of accurate and complete domain name registration data, TLD registries and the entities providing domain name registration services for the TLD (so-called registrars) should collect and guarantee the integrity and availability of domain names registration data. In particular, TLD registries and the entities providing domain name registration services for the TLD should establish policies and procedures to collect and maintain accurate and complete registration data, as well as to prevent and correct inaccurate registration data in accordance with Union data protection rules.

(62) TLD registries and the entities providing domain name registration services for them should make publically (sic) available domain name registration data that fall outside the scope of Union data protection rules, such as data that concern legal persons. TLD registries and the entities providing domain name registration services for the TLD should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, in accordance with Union data protection law. Member States should ensure that TLD registries and the entities providing domain name registration services for them should respond without undue delay to requests from legitimate access seekers for the disclosure of domain name registration data. TLD registries and the entities providing domain name registration services for them should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. The access procedure may also include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission may adopt guidelines on such procedures without prejudice to the competences of the European Data Protection Board.

(…)

69. The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by entities, public authorities, CERTs, CSIRTs, and providers of security technologies and services should constitute a legitimate interest of the data controller concerned, as referred to in Regulation (EU) 2016/679. That should include measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Such measures may require the processing of the following types of personal data: IP addresses, uniform resources locators (URLs), domain names, and email addresses.”

Recitals 59-62 inclusive are then broadly mirrored in Article 23 of the draft NIS2 Directive.

Recitals 15, 59-61 inclusive, and 69, and Articles 23(1-3) of the draft NIS2 Directive, are broadly supportive of complete, fulsome registration data processing, provided it is GDPR-compliant. The final sentence of Recital 61 also expressly supports measures designed to promote compliance with the GDPR’s accuracy principle, such as those mentioned in our previous memoranda.

However, Recital 62, and Articles 23(4-5), are more specifically relevant to the matters under discussion in this memorandum, as they concern the publication/dissemination of registration data, not just its mere collection and retention. Those provisions of the NIS2 Directive draw a clear distinction between personal and non-personal data, and only expressly support the publication of non-personal data. In respect of personal data, the NIS2 Directive limits itself to discussing what appears to be *restricted* access by “legitimate access seekers, in accordance with Union data protection law” (and equivalent wording in Article 23(5)).

In our view, therefore, the current draft NIS2 Directive does not appear to consider a system in which some personal data may (legitimately) be openly published, e.g. with a Registrant’s consent. It is not clear whether this just because that option was not considered by the drafters, *or* because the drafters did not consider such an approach to be worthwhile and/or compliant. However, it means that the current draft NIS2 Directive does not offer significant support/risk-reduction for a system premised on, for example, Registrant consent (though nor does it expressly undermine such an approach).

\* \* \*

1. EDPB Letter to Göran Marby dated 5 July 2018; available online at <https://edpb.europa.eu/sites/default/files/files/news/icann_letter_en.pdf> [↑](#footnote-ref-1)
2. Other references to wider interests do not discuss sharing Registrant data with them. For example, Recital 20 says “[t]he Registry should adopt clear policies aiming to ensure the timely identification of abusive registrations of domain names and, where necessary, should cooperate with competent authorities and other public bodies relevant to cybersecurity and information security which are specifically involved in the fight against such registrations, such as national computer emergency response teams (CERTs).” “Cooperation” *could* entail sharing of personal data, but (perhaps deliberately), the new .EU Regulation is silent on this point. [↑](#footnote-ref-2)
3. We have not been able to confirm this; the current [EURid privacy notice](https://eurid.eu/en/other-infomation/privacy-policy/) does not specifically state what GDPR legal basis justifies the publication of registration data , though it does state that “We are required to maintain a complete and accurate database of all registered Domain Names. The purpose of the WHOIS look-up facility (<https://whois.eurid.eu/en/> is to provide accurate and up-to-date information about the technical and administrative contact persons administering the Domain Names. This helps us in creating and maintaining a trusted and safe Internet environment.” The reference to publications being “required” seems consistent with either GDPR Article 6(1)(e) (public task) *or* Article 6(1)(c) (legal obligation). [↑](#footnote-ref-3)
4. We note with interest that the question posed asserts that EURid invokes GDPR Article 6(1)(e) – task in the public interest / public authority – *not* GDPR Article 6(1)(f), legitimate interests. EURid is not a public authority, so it is in principle capable of invoking legitimate interests for its publication of personal data. We are not privy to EURid’s reasoning for avoiding the “legitimate interests” basis, and therefore cannot offer substantial comment on this observation; that said, it might not be helpful/reassuring for other Contracted Parties; unlike EURid, most Contracted Parties cannot rely on GDPR Article 6(1)(e) because, unlike EURid, there is no EU or Member State law underpinning their own WHOIS-related processing. [↑](#footnote-ref-4)
5. E.g. Recital 11 of the New .EU Regulation states: “The Commission should enter into a contract with the designated Registry, which should include the detailed principles and procedures that apply to the Registry for the organisation, administration and management of the .eu TLD.” [↑](#footnote-ref-5)
6. “The mere fact that a registrant is a legal person does not necessarily justify unlimited publication of personal data relating to natural persons who work for or represent that organization, such as natural persons who manage administrative or technical issues on behalf of the registrant. For example, the publication of the personal email address of a technical contact person consisting of firstname.lastname@company.com can reveal information regarding their current employer as well as their role within the organization. Together with the address of the registrant, it may also reveal information about his or her place of work.” EDPB July 2018 Letter, at page 5. [↑](#footnote-ref-6)
7. EDPB July 2018 Letter, at pages 2-3. [↑](#footnote-ref-7)