MEMORANDUM

|  |  |
| --- | --- |
| **To:** | Internet Corporation for Assigned Names and Numbers (ICANN), EPDP Team |
| **From:** | Ruth Boardman & Katerina Tassi, Bird & Bird LLP |
| **Date:** | 13 March 2020  |
| **Subject:** | Advice on consent options for the purpose of making personal data public in RDS and requirements under the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**")  |

|  |
| --- |
| **EXECUTIVE SUMMARY**This document analyses the consent requirements set out in the GDPR and examines consents options for the purpose of publishing in RDS personal data provided in the context of the registration of legal person registrants. Consent requirementsPursuant to the GDPR, consent must be freely given, specific, informed and unambiguous. Also, it needs to be obtained prior to the processing taking place. Controllers must be able to demonstrate that valid consent has been given and individuals have the right to withdraw consent at any time. Under the GDPR, the obligation to obtain consent lies with the controller. The controller may instruct a third party to obtain consent from individuals on its behalf; however, doing so will not relieve the controller from its obligations under the GDPR. Consent optionsOn the basis of the above requirements, this documents examines the following options of obtaining consent for making personal data public in RDS and sets out the compliance considerations of each option:1. Controllers seek valid consent directly from individuals
* Making personal data public in RDS is optional.
* Prior to making personal data public, the controller contacts individuals directly to seek consent in line with the GDPR.
* In the event of refusal to consent or failure to respond, the personal data will not be made public.
1. Registrant obtains valid consent and provides evidence to controller
* Making personal data public in RDS is optional.
* Prior to making personal data public, the controller requires the registrant to:

(a) obtain individuals' consent; and (b) provide to the controller evidence that consent has been obtained.* In the event of refusal to consent or failure to receive evidence, the personal data will not be made public.
1. Registrant obtains valid consent and controller confirms this with the individual
* Prior to making personal data public, the controller requires the registrant to:

(a) obtain individuals' consent; and (b) provide to the controller evidence that consent has been obtained.* Controller follows up with the individual directly: it informs them that the registrant has confirmed they have granted consent.
1. Registrant undertakes the obligation to obtain consent
* Registrants are allowed to provide non-personal contact details.
* Registration data is made public by default (irrespective of whether or not personal data is included).
* By means of a statement, registrants undertake to ensure they have obtained individuals' consent if they choose to provide personal data.

  |

**Question presented**

Registration data submitted by legal person registrants may contain the data of natural persons. A Phase 1 memo stated that registrars can rely on a registrant's self-identification as legal or natural person if risk is mitigated by taking further steps to ensure the accuracy of the registrant's designation.

As a follow up to that memo: what are the consent options and requirements related to such designations? Specifically: are data controllers entitled to rely on a statement obligating legal person registrants to obtain consent from a natural person who would act as a contact and whose information may be publicly displayed in RDS? If so, what representations, if any, would be helpful for the controller to obtain from the legal person registrant in this case?

As part of your analysis please consult the GDPR policies and practices of the Internet protocol (IP address) registry RIPE-NCC (the registry for Europe, based in the Netherlands). RIPE-NCC's customers (registrants) are legal persons being displayed publicly in WHOIS. RIPE-NCC places the responsibility on its legal-person registrants to obtain permission from those natural persons, and provides procedures and safeguards for that. RIPE-NCC states mission justifications and data collection purposes similar to those in ICANN's Temporary Specification. Could similar policies and procedures be used at ICANN?

Also see the policies of ARIN, the IP address registry for North America.  ARIN has some customers located in the EU.  ARIN also publishes the data of natural persons in its WHOIS output.  ARIN’s customers are natural persons, who submit the data of natural person contacts.

**Introduction**

1. Background: Previous advice provided by Bird & Bird (“Phase 1 memo”) examined liability in connection with a registrant’s self-identification as a natural or non-natural person pursuant to the GDPR. This Phase 1 memo examined the approach of: (i) distinguishing registrants whose registration data does not include any personal data (“non-personal registrants”) from those that provide personal data and (ii) by default making public the registration data of the former. Self-identification of registrants and additional measures for distinguishing non-personal registrants were examined in the Phase 1 memo.
2. Objective of this memo: This document focusses on the use of consent as a lawful basis for making public in the Registration Directory Service ("RDS") personal data of admin/ tech contacts provided by a legal person registrant. It does not examine further the means by which controllers would identify whether personal data is contained in the registration data.
3. Furthermore, this document does not examine points such as the transfer of registration data to the registry and escrow provider, the legitimate character of publishing data in RDS or the elements of registration data which should be published in RDS. We appreciate that these matters have been separately examined by EPDP; we have therefore not addressed these points.
4. As requested, we have taken into account the policies followed by RIPE-NCC and by ARIN. Our comments in relation to RIPE-NCC policies are included in para 15 below. In respect of ARIN, we note that ARIN consider that they are not in principle subject to the GDPR: the article "Personal Data Privacy Considerations at ARIN"[[1]](#footnote-1) published by the ARIN President & CEO and the ARIN General Counsel states that "*ARIN's general operational activities do not fall within the scope of GDPR*" and takes the view that the GDPR could be relevant only to "incidental activities" (for example, event registration).
5. Structure: This document provides relevant background information and examines the following points:
* The concept of consent as a lawful basis for making personal data publicly available in RDS and the parties responsible for obtaining consent (paras 10-12);
* the elements of valid consent under the GDPR (paras 13-18);
* additional GDPR requirements relating to consent, such as the requirement to demonstrate consent and the right of individuals to withdraw consent at any time (paras 19-23); and
* options for consent in the RDS context (para 24).

**Analysis**

1. This document examines the processing of *personal* data in the context of RDS. By way of clarification, registration data of legal person registrants includes personal data when the contact details relate to a natural person (such as firstnamelastname@company.com). Generic contact details of legal persons (such as info@company.com) do not constitute personal data and are not examined in this document as they do not trigger GDPR concerns.
2. By way of background, the EDPB and its predecessor, the Article 29 Working Party ("WP29") have examined -in previous communications with ICANN- the point of making personal data public in WHOIS. In its letter of 05 July 2018[[2]](#footnote-2), the EDPB considered that "*registrants should in principle not be required to provide personal data directly identifying individual employees or third parties fulfilling the administrative or technical functions on behalf of the registrant*”.
3. In the same letter, the EDPB stated that “*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*”. On this basis, the EDPB considered 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*”.
4. EPDP Phase 2 Legal Committee's consideration that controllers would rely on individuals' consent as a lawful basis for making their contact details public in the RDS is in principle in line with the above views.
5. Compliance with Lawfulness principle: Pursuant to the Lawfulness, fairness and transparency principle (under Article 5(1)(a) GDPR), personal data shall be processed only and to the extent that at least one of the lawful bases set out in Article 6 GDPR applies. Consent - set out in Article 6(1)(a) GDPR – constitutes one of these bases.
6. Under the GDPR (Article 5(2)), the party that bears the responsibility of establishing a lawful basis for the processing of personal data is the controller: subsequently, where consent applies, the controller will be responsible for obtaining such consent in line with GDPR requirements. This is also confirmed by Article 7(1) GDPR, which requires controllers to be able to demonstrate consent.
7. Controllers cannot be discharged from their obligation to establish a lawful basis – and obtain valid consent – by means of contractual arrangements with registrants. This is an important point to note as, irrespective of how controllers will obtain consent, they will ultimately be responsible for complying with the lawfulness principle and they will have to be able to demonstrate such compliance.
8. Consent requirements: To be valid, consent must meet GDPR standards – as per Article 4(11) GDPR, it must be freely given, specific, informed and unambiguous. The request for consent shall be clearly distinguishable from other matters, for example, contractual terms, and individuals shall have the right to withdraw consent at any time (Article 7(2) & (3) GDPR). Each of these elements is examined further below.
9. Freely given: Individuals must have a genuine choice as to whether or not they provide consent and they must be able to refuse or withdraw consent without detriment[[3]](#footnote-3). Two points are of particular relevance to the case examined in this document: imbalance of power and conditionality.
	1. Imbalance of power: We appreciate that in many cases legal person registrants will appoint their employees as admin/tech contacts and will provide their contact details. Due to the imbalance of power that occurs in the employment context, seeking consent from employees can be problematic, as it is unlikely to be freely given[[4]](#footnote-4). However, the EDPB recognises that employees can give free consent – albeit in limited circumstances – when it will have no adverse consequences at all whether or not they give consent. Given the higher bar to prove that consent is freely given, when obtaining consent for making data public in the RDS, it should be ensured and made clear to individuals that they have a genuine option to choose whether or not their information will be published and that refusing to consent will have no impact on them.
	2. Conditionality: Article 7(4) GDPR indicates that when assessing whether consent is freely given, "*utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract*". We acknowledge that in the context of RDS it is the legal person registrant, and not the individual, who enters into a contract with controllers and receives their domain name registration services. Although Article 7(4) may more typically be applied in situations when the data subject wishes to receive services from the controller, it is drafted in more general terms and is not restricted to situations when the data subject is to receive the services. If contact details of natural persons acting as admin/tech contacts for legal person registrants is to be made public by default, and if legal person registrants are required to obtain consent from the relevant points of contact for this, then it will be prohibitively difficult to rebut the presumption, set out at Article 7(4) that the consent is not be freely given. If the legal person registrant does not have the option to keep contact details non-public or to have contact details removed from RDS without replacing them with other contact details, then this lack of option will likely impact on individuals' freedom to refuse/withdraw consent and the unconditional character of these rights.
10. In this respect, we note that the question analysed in this document points to the RIPE-NCC registry. On the basis of the information provided on the RIPE-NCC webpages shared with us, we note that RIPE-NCC purport to rely on consent when an individual other than the "resource holder" is appointed as point of contact and require the "resource holder" to obtain consent from that individual. We also note that the publication of the point of contact's details is mandatory; thus, registration is conditional on the "resource holder" ensuring consent from the person they wish to appoint as point of contact. In our view, this practice triggers the presumption examined above, that in this context consent will not be freely given.
11. Specific: Pursuant to Article 6(1)(a) GDPR, consent must be given in respect of the processing of data "*for one or more specific purposes*". As the EDPB consent guidelines mention, "*obtaining valid consent is always preceded by the determination of a specific, explicit and legitimate purpose for the intended processing activity*". This means that consent should be sought for the particular processing operation, i.e. the publication of individuals' contact details in the RDS (and individuals should be made specifically aware of this purpose).
12. Informed: Providing information to individuals prior to obtaining their consent is a key requirement to ensure that they are in a position to make informed decisions and thus provide valid consent. Pursuant to the EDPB consent guidelines, controllers shall provide to individuals at least the following information prior to obtaining their consent:
* The identity of the controller(s);
* The purpose for which consent is sought;
* The type of data collected and used;
* The existence of the right to withdraw consent;
* Where relevant, information about the use of the data for automated decision-making in accordance with Article 22(2)(c) GDPR;
* Where relevant, information on the possible risks of data transfers due to the absence of an adequacy decision and of appropriate safeguards as described in Article 46 GDPR.

In line with the requirements of Article 12 GDPR, the information should be provided in clear and plain language. To ensure that individuals receive adequate information in an appropriate form, we suggest that controllers always have control over the language to be used in such an information notice.

1. Unambiguous: Consent requires a statement by the individual or a clear affirmative act, which demonstrates that individuals must have taken a deliberate action to consent to a particular processing. For example, merely informing an individual that their contact details will be made public unless they object, does not constitute an unambiguous indication of their wishes and thus does not equal valid consent.

1. Timing of consent: Consent needs to be obtained prior to the relevant processing operation taking place. Although this is not expressly stated in the GDPR, the EDPB consent guidelines consider this is implied by the wording used in Article 6(1)(a) GDPR ("the data subject *has given* consent […]").
2. Demonstrating consent: Pursuant to the accountability principle set out in Article 5(2) GDPR and Article 7(1) GDPR the controller must be able to demonstrate that individuals have consented. The GDPR does not prescribe how this requirement is to be met. Pursuant to the French Data Protection Authority ("CNIL"), consent must be documented in a way that allows the controller to demonstrate the free and unambiguous character of consent, as well as that the different purposes for which consent was granted were clearly distinguished and that individuals were appropriately informed[[5]](#footnote-5). Other supervisory authorities have also provided guidance on this topic[[6]](#footnote-6).

From a practical perspective, if a complaint is raised with a supervisory authority, the latter would most likely request the controller to provide a record of consent.

1. Withdrawal of consent: Individuals have the right to withdraw their consent and it should be as easy to do so as it was to provide consent in the first place (Article 7(3) GDPR). This is an unconditional right which individuals can exercise at any time. Hence, controllers should have in place a procedure to (a) allow individuals to exercise this right (for example, provide for a relevant contact), and (b) to ensure that the contact details of individuals who withdraw consent are removed from the RDS.
2. Consent renewal: Although the GDPR does not specifically impose the obligation to renew consent, EDPB consent guidelines recommend – as a best practice – to refresh consent at appropriate intervals. If processing of operations change or evolve considerably, then the original consent will no longer be valid; in such case, new consent will need to be obtained. This is a point that EPDP might want to explore further, in particular in conjunction with any measures to ensure the accuracy of the data.
3. Consent via a third party: GDPR does not prescribe that consent needs to be sought from individuals directly by the controller. As long as controllers can ensure that the above requirements are met, they could task the registrant to obtain consent for their purposes. We appreciate this might be a more practical option given the relationship that registrants are expected to have with their admin/tech contacts (employment or other contractual relationship). As explained above, instructing a third party to obtain consent on the controllers' behalf will not relieve the latter from their obligations under the GDPR. If the registrant fails to obtain valid consent, the controller will also not have valid consent; rather it will have a claim for breach of contract against the registrant. This is further examined below.
4. Consent options: In light of the above considerations, we examine below a series of options, each at a different level on the compliance scale.

|  |  |  |
| --- | --- | --- |
| **No.** | **Option** | **Compliance considerations** |
|  | Controllers seek valid consent directly from individuals* Making personal data public in RDS is optional.
* Prior to making personal data public, the controller contacts individuals directly to seek consent in line with the GDPR requirements examined above (consent wording provides adequate information in line with para 17 above, is specific to the processing operation of making the data public in RDS, explains clearly that individuals are free to say no and doing so will have no impact on them (or the registration process), and informs individuals on how they can withdraw consent if they wish to).
* The communication makes available to individuals the controller's privacy notice (for example, via a hyperlink).
* Granting consent is recorded for evidential purposes.
* In the event of refusal to consent or failure to respond, the personal data will not be made public.
 | Seeking consent directly from individuals is the safest option as controllers will have control over the consent process, will be in a position to ensure that consent is obtained in accordance with GDPR standards and that they meet their transparency obligations. Also, it allows them to manage withdrawals of consent and promptly act upon these. Finally, in line with their accountability obligations, controllers will be able to demonstrate that valid consent has been obtained by keeping records of consent.  |
|  | Registrant obtains valid consent and provides evidence to controller* Making personal data public in RDS is optional.
* Prior to making personal data public, the controller requires the registrant to:

(a) obtain individuals' consent using a consent method defined by the controller (for example, consent form with specific wording and format which meets GDPR requirements); and (b) provide to the controller evidence that consent has been obtained (for example by means of the registrant providing a signed copy of the consent form or the individual directly forwarding this to controller). * In the event of refusal to consent or failure to receive evidence, the personal data will not be made public.
 | As an alternative to the above option, controllers can require the registrant to:(a) obtain valid consent on their behalf –using an approved consent method and wording- and(b) provide proof of such consent.This way, controllers still maintain control over the consent process and are in a position to verify whether consent has been validly obtained.The method is somewhat less robust than option 1, as the controller does not receive direct confirmation from the data subject that he or she has given consent. In the (possibly rare) situation that the registrant does not obtain consent from the admin/ tech contact, then the consent would not be valid. |
|  | Registrant obtains valid consent and controller confirms this with the individual* Making personal data public in RDS is optional.
* Prior to making personal data public, the controller requires the registrant to:

(a) obtain individuals' consent using a consent method defined by the controller (for example, consent form with specific wording and format which meets GDPR requirements); and (b) provide to the controller evidence that consent has been obtained (for example by means of the registrant providing a signed copy of the consent form or the individual directly forwarding this to controller). * Controller follows up with the individual directly: it informs them that the registrant has confirmed they have granted consent. The controller advises the individual to let them know if this confirmation has been provided erroneously and that in absence of a response from their side, the personal data will be made public within [x time]. The controller can also use this opportunity to provide all information to be made available to the individual, incl. in relation to their right to withdraw consent.
 | This option is a variant of option number 2 – in addition to receiving evidence of consent, the controller contacts individuals directly to confirm consent. This places a higher administrative burden on the controller, but would mitigate the risk that the registrant has not actually secured consent from the relevant person.  |
|  | Registrant confirms they have obtained valid consent and undertakes the obligation to provide a copy if requested* Making personal data public in RDS is optional.
* Prior to making personal data public, the controller requires the registrant to:

(a) obtain individual's consent using a consent method defined by the controller (for example, consent form with specific wording and format which meets GDPR requirements); and (b) confirm that they have done so. * In addition, controller undertakes the obligation to keep copies of consent and provide to controller if requested.
 | Under this option, there is less control over the consent process compared to the above options and more reliance on the registrant to comply with their –contractual- obligations. The obligations undertaken by the registrant may provide the controller with a contractual recourse against the registrant. However, the controller will not be discharged from its obligations under the GDPR and – if the registrant has not met its obligations and/or does not provide a copy of the consent on request – then the controller will not be able to demonstrate that consent requirements are met, so this will impact on controller's compliance with GDPR.  |
| 1.
 | Registrant undertakes the obligation to obtain consent* Registrants are allowed to provide non-personal contact details; however, registration data is made public by default (irrespective of whether or not personal data is included).
* By means of a statement, registrants undertake to ensure they have obtained individuals' consent if they choose to provide personal data.
 | This option is unlikely to be GDPR-compliant for a number of reasons:* The controller has taken no action to ensure that consent has been obtained, although the obligation to obtain consent continues to rests with the controller;
* Also, the controller is not in a position to demonstrate compliance with Article 4(11) and Article 7 GDPR requirements or with its transparency obligation.
* The controller does not hold any record of consent.
* Consent will not be freely given as individuals are not in a position to effectively exercise their –unconditional- right to withdraw consent: since the publication of contact details is mandatory, withdrawing consent will be subject to the registrant providing alternative contact details.
 |

1. Available here: <https://teamarin.net/2018/03/20/personal-data-privacy-considerations-at-arin/> [↑](#footnote-ref-1)
2. Letter from Andrea Jelinek to Goran Marby in reply to his 10 May 2018 letter, available here: <https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf>. [↑](#footnote-ref-2)
3. Recital 42 GDPR and Article 29 Working Party Guidelines on consent under Regulation 2016/679 as last revised and adopted on 10 April 2018 and endorsed by EDPB on 25 May 2018 ("**EDPB consent guidelines**"). [↑](#footnote-ref-3)
4. EDPB consent guidelines (page 7) and ICO's guidance on consent (available here:

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/>) [↑](#footnote-ref-4)
5. <https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes> [↑](#footnote-ref-5)
6. For example, the [Belgian Data Protection Authority](https://www.gegevensbeschermingsautoriteit.be/node/21004) confirms that for consent to be valid the controller itself must record consent, including the information on which such consent was based. The ICO's consent guidance also examines this point and mentions that controllers must have an effective audit trail of how and when consent is given and should be able to provide evidence if challenged. Pursuant to the ICO, records of consent must demonstrate the following: who consented, when they consented, what they were told at the time, how they consented and whether they have withdrawn consent. [↑](#footnote-ref-6)