ICANN org comments on the Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the EU, repealing Directive (EU) 2016/1148 (NIS 2 Directive)

1. About the Internet Corporation for Assigned Names and Numbers (ICANN) and Summary of Comments

The Internet Corporation for Assigned Names and Numbers (ICANN) is a not-for-profit public-benefit corporation that, on behalf of the Internet community, oversees the technical coordination of the top-most level of the Internet's Domain Name System (DNS), and especially its security, stability, and resiliency.

ICANN brings together governments, non-commercial and commercial stakeholder groups, civil society, and individuals. Each group represents a different interest on the Internet. Collectively, they make up the ICANN community, which develops policies for the DNS through a consensus-driven bottom-up process.

ICANN is headquartered in Los Angeles and has regional offices in Brussels, Istanbul, Montevideo, and Singapore. ICANN also has engagement centers in Washington, D.C., Geneva, Beijing, and Nairobi.

ICANN org submits this comment on the Proposal for a Directive on Measures for a High Common Level of Cybersecurity Across the EU, repealing Directive (EU) 2016/1148 (NIS 2 Directive), in recognition of the far-reaching impacts this directive could have on the DNS. We would like to emphasize two issues, as discussed in greater detail below.

First, ICANN org believes that the reach of the NIS 2 Directive's scope of application to DNS service providers is overly broad. ICANN org would urge policymakers to reconsider the qualification of different DNS service providers as essential entities and consider the implementation of certain threshold criteria for DNS service providers to qualify as essential or important entities. One potential suggestion could be to distinguish between providers of authoritative domain name resolution services and providers of recursive domain name resolution services as DNS service providers.

Second, with respect to the proposed requirements concerning domain name registration data in Art. 23 NIS 2 Directive, ICANN org suggests that such requirements should be set out with greater clarity. The requirements of the European Union (EU) General Data Protection Regulation (GDPR) have had a significant impact on the personal data processing activities of the whole Internet community. Therefore, ICANN org welcomes the intention of the European Commission to legally acknowledge the important role that providers of DNS services are playing for the security, stability, and resilience of the DNS and to balance the interests between the security, stability, and resilience of the DNS with the need for protection of personal data and privacy. Added specificity in this section could help to ensure the

availability of accurate and complete domain name registration data and to provide efficient access to domain name registration data for legitimate access seekers.

ICANN org would like to reference the ICANN community's extensive policy-making efforts concerning gTLD registration data, particularly since the GDPR went into effect. Notably, the ICANN community has recommended the implementation of consensus policy requirements for gTLD registrars and registry operators to collect a specific set of registration data elements (as identified in point c below).[1] These consensus policies could help to inform efforts to close some of the gaps ICANN org has identified in Art. 23 NIS2 Directive, for example, a need to specify what registration data elements should be required to make such data "complete."

2. Concerns Regarding the NIS 2 Directive's Broad Scope

The scope of the NIS 2 Directive is set out in its Art. 2. ICANN org brings to the attention of the European Commission that this scope is overly broad, particularly as applied to DNS service providers.

Micro and small enterprises, within the meaning of Commission Recommendation 2003/361/EC, are explicitly not in scope per Art. 2(1) NIS 2 Directive. Art. 2(1) NIS 2 Directive, however, brings micro and small enterprises back in scope if they are classified as DNS service providers, as referred to in point 8 of Annex I.

Art. 4 (14) NIS 2 Directive classifies a "DNS service provider" as an entity that provides either recursive or authoritative domain name resolution services to Internet end users or other DNS service providers. Recital 15 states that this directive should apply to all providers of DNS services in the DNS resolution chain, both recursive resolvers and operators of authoritative servers for the root zone, for top level domains, and for all other levels of the name tree. This is an extremely broad scope.

The domain name system consists of two conceptually independent systems: the publication side (referred to as "authoritative domain name resolution services" in Art. 4 (14) NIS 2 Directive), and the resolving side (referred to as "recursive domain name resolution services to Internet end users or other DNS service providers" in Art. 4 (14) NIS 2 Directive).

The publication side includes the authoritative name servers: the root name servers are authoritative for the root zone, top level domain name servers for TLD zones, and so on. This can be viewed as an inverted tree structure, with the root at the top. In a simplified view, all authoritative name servers are part of this single tree, and all authoritative name servers provide a service to the Internet by making their data available. This service may be offered to persons

[1] See Final Report of the Expedited Policy Development Process on the Temporary Specification for gTLD Registration Data, at Recommendation 5, https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf.

in the 27 EU Member States as well, making all these authoritative name servers, regardless of location, ownership, or content, potentially subject to the NIS 2 Directive, pursuant to Art. 2(2).

The consuming side of the domain name system is the part that uses (resolves) the data, published by the authoritative name servers, to find information such as Internet addresses belonging to a domain name. In a simplified view, recursive resolvers traverse the DNS tree, from the root to the leaves, on behalf of the end users. However, the reality is far more complex. Recursive resolvers that traverse the DNS tree can work on behalf of forwarders, which forward DNS requests on behalf of specific applications or end users. Often, multiple forwarders or recursive resolvers are involved in resolving a single domain name. Recursive resolvers may have various strategies to resolve names more efficiently, which may depend on the topological location of the authoritative servers involved. In short, at any point during a name resolving process, a forwarder, recursive resolver, authoritative name server, or a domain name may be involved that is associated with an entity in any of the 27 EU Member States.

Many entities such as sole traders, partnerships, private limited companies, charities, community groups, social enterprises, and individuals fall into the NIS 2 Directive's category of essential entities if they host their own domain name or help others with such hosting. For clarity, when we refer to hosting a domain name we refer to operating its authoritative name servers. To illustrate the size of the scope relating to hosting a domain, currently more than 46 million domain names are registered under TLDs (known as country code TLDs) that represent the country names of the 27 EU Member States, while many entities in the 27 EU Member States host domain names that are registered outside these country code top-level domains.

Additionally, many of the aforementioned entities operate their own recursive resolvers to serve their members and employees. To illustrate the size of the scope relating to recursive resolvers, more than 6 million individual recursive resolver addresses query the ICANN Managed Root Server (IMRS) daily. At least 22% of these addresses are allocated to entities in the EU.

The entities that operate authoritative name servers or recursive resolvers, often not otherwise classified as essential or important, are currently deemed in scope of the NIS 2 Directive simply because they host a domain name or operate a recursive resolver. This classification would lead to additional administrative burdens and compliance costs that would act as a deterrent to hosting a domain or operating a recursive resolver, which increases the threshold of participation in online presence and increases their dependency on third-party hosting and resolving services.

One specific authoritative domain name resolution service to note is that of root name service. Given the tree-like structure of the domain name system, the root of the DNS is a critical component of all domain name resolutions: the vast majority of recursive resolvers begin the resolution process of any domain name by obtaining "referral" information for top-level domain name servers from one of 13 root server "identities" (implemented using 13 IPv4

and 13 IPv6 addresses on over 1,000 individual machines globally). While this service, available to all users of the DNS regardless of location, has operated since the creation of the DNS in the mid-1980s without a single period of end user-visible interruption, root name service is provided by 12 independent organizations around the world on a voluntary basis at no cost to the users of that service. That is, the 12 independent organizations, which include RIPE-NCC in the Netherlands and Netnod in Sweden, provide root name service for the greater good of all Internet users, not for revenue. If undue, and in 10 of 12 cases, extra-territorial, regulatory oversight were to be applied by the EU, it is possible such voluntary service would no longer be feasible, resulting in a potential fundamental restructuring of how root name service is provided with unknown long-term consequences.

Therefore, ICANN org would welcome a discussion about the scope of DNS providers qualifying as essential or important entities and the implementation of certain threshold criteria for DNS service providers to qualify as essential or important entities.

A possible avenue that may be pursued in this regard could be to distinguish between providers of authoritative domain name resolution services and providers of recursive domain name resolution services as DNS service providers.

Providers of authoritative domain name resolution services should only qualify as essential entities if they serve domains of essential or important entities. Ideally, the qualification as an essential or important entity would follow the qualification of the entity for which the provider of authoritative domain name resolution services serves the domain. In other words, if the provider of an authoritative domain name resolution service serves the domain of one or more entities qualifying as essential entities, the provider of authoritative domain name resolution services would also qualify as essential entity. Whereas the provider of authoritative domain name resolution services would only qualify as an important entity, if it serves the domain of one or more important entities.

For providers of recursive domain name resolution services, a meaningful differentiation between DNS providers qualifying as an essential entity could be made by making such qualification dependent upon whether the end user is left with a choice, in other words whether the end user is required to use a particular provider of recursive domain name resolution services or not.

ICANN org would welcome if these suggestions could serve as a basis for a further discussion on how to reasonably qualify DNS service providers as important or essential entities for ensuring a high common level of cybersecurity in the EU.

3. Databases of Domain Names and Registration Data

a. Publication of Domain Name Data That Fall Outside the Scope of EU Data Protection Rules

Art. 23 (4) and Recital 62 of the NIS 2 Directive require Member States to ensure that top-level domain (TLD) registries and the entities providing domain name registration services for the TLD publish available domain name registration data that fall outside the scope of EU data protection rules, in particular data concerning legal persons, without undue delay after the registration of a domain name.

In this regard, ICANN org wants to bring to the attention of the European Commission (EC) that even presumably non-personal data such as the legal persons' name may contain data that are to be considered personal data under EU data protection rules.[2] The European Data Protection Board (EDPB) emphasized this in a 5 July 2018 letter to ICANN org,[3] stating that "[t]he 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." Thus, Art. 23 (4) and Recital 62 raise a critical question: How should a differentiation between personal and non-personal data be accomplished? In addition, how would liability under EU data protection law be allocated if personal data are mistakenly published in this process?

To provide efficient access to domain name registration data for legitimate access seekers as required under the NIS 2 Directive, TLD registries and the entities providing domain name registration services must be able to automate such publication process to at least some degree.

Therefore, ICANN org would welcome additional clarification in the NIS 2 Directive regarding the circumstances, including specification of the potentially sufficient technical and organizational measures, in which publication in a GDPR and NIS 2 Directive-compliant manner could be achieved, and which data categories such publication should cover. Would it, for example, suffice to require registrants to confirm that data categories such as domain name, legal person name, and contact details do not include personal data (for example, via a "check the box" mechanism")? Consequently, domain name registration data, including domain names and names of legal persons, would only be published if registrants confirm that these data categories exclude personal data? Furthermore, the specification of the potentially sufficient technical and organizational measures to publish registration data should enable TLD registries

[2] Cf. Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive of the European Data Protection Supervisor, p. 12 et seq.: "*The EDPS equally recommends clarifying in greater detail which categories of data domain registration data (which do not constitute personal data) should be the subject of publication.*"
[3] See 5 July 2018 letter from EDPB to ICANN org at https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf.

and the entities providing domain name registration services for the TLD to demonstrate compliance with the NIS 2 Directive and implicitly the requirements of the GDPR on technical and organizational measures when personal data have been mistakenly marked by the registrant as not containing personal data and have therefore been published.

Another possible way to achieve the purpose of providing efficient access to domain registration data for legitimate access seekers in balance with the right to data protection and privacy would be to require Member States in the NIS 2 Directive to ensure that TLD registries and the entities providing domain name registration services for the TLD publish certain specified domain name registration data of legal persons (such as domain name and legal person name) regardless of whether such data contains personal data, taking into account that the potential encroachment upon the right to data protection and privacy with respect to such otherwise typically publicly available data categories is minimal and is therefore justifiable on the basis of legitimate interests. To prevent any misunderstanding, it should furthermore be clarified with regard to Art. 23(4) GDPR in connection with Recital 62 NIS 2 Directive that such publication requirement is a legal obligation for TLD registries and the entities providing domain name registration services for the TLD in terms of Art. 6 (1) c, and Art. 6(3) GDPR. This would legitimize the publication of certain specified domain name registration data of legal persons (such as domain name and legal person name) under Member State law, even in cases where such data categories contain personal data.

b. Provide Access to Specific Domain Name Registration Data Upon Lawful and Duly Justified Requests of Legitimate Access Seekers

Art. 23 (5) in connection with Recital 62 of the NIS 2 Directive requires Member States to ensure that TLD registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data concerning natural persons to legitimate access seekers upon lawful and duly justified requests. This is similar to the current requirements concerning the provision of access to nonpublic gTLD registration data by gTLD registry operators and registrars under ICANN's Interim Registration Data Policy for gTLDs.[4]

To enable TLD registries and the entities providing domain name registration services for the TLD to provide access to specific domain name registration data concerning natural persons to legitimate access seekers with the required legal certainty, it should be clarified that the national law of the Member States implementing the NIS 2 Directive requirement shall serve as a legal obligation in terms of Art. 6 (1) c, and Art. 6(1)(3) GDPR, for example by explicitly stipulating this in Recital 62 and by deleting the passage "*in compliance with Union*

[4] See Interim Registration Data Policy for gTLDs (extending applicability of Temporary Specification for gTLD Registration Data), at https://www.icann.org/resources/pages/interim-registration-data-policy-en#:~:text=This%20Interim%20Registration%20Data%20Policy,%2Dlevel%20domains%20(gTLDs). For specific requirements concerning access to non-public gTLD registration data, see Temporary Specification, at Annex A, Section 4, https://www.icann.org/resources/pages/gtld-registration-data-specs-en/#appendixA.

data protection law" in Art. 23 (5) NIS 2 Directive. Further specifics surrounding this legal obligation would also need to be defined.

The addition "*in compliance with Union data protection law*" may be unnecessary. The GDPR applies to TLD registries and the entities providing domain name registration services for the TLD processing personal data contained in domain name registration data if this processing falls within the territorial scope of the GDPR, irrespective of whether this is provided for under the NIS 2 Directive or not. The addition "*in compliance with Union data protection law*" might be interpreted as stipulating an additional requirement for providing access to domain name registration data pursuant to Art. 23 (5) NIS 2 Directive. This would have the consequence that TLD registries and the entities providing domain name registration services for the TLD could not rely on Art. 6 (1) c GDPR for the provision of access to domain name registration data containing personal data.

In this scenario, TLD registries and the entities providing domain name registration services for the TLD would have to carry out a weighing of interests pursuant to Art. 6 (1) f GDPR, to determine whether they may provide access to legitimate access seekers. This would not only hinder the provision of access to domain name registration data in some cases, but also significantly slow down the process to provide access. This becomes even more apparent when taking into account the following aspects, which impair the goal of providing efficient access to domain name registration data for lawful access seekers:

- It is not clear under Art. 6 (1) f GDPR whether and to which extent use cases can be established for the weighing of interests, or whether a weighing must be carried out in every individual case, thereby requiring a new assessment for every single request.
- It is not clear whether the automated provision of access would constitute automated individual decision-making under Art. 22 GDPR and therefore would be prohibited if publication is based on Art. 6 (1) f GDPR.

Additionally, to provide efficient access to domain name registration data containing personal data for lawful access seekers, TLD registries and the entities providing domain name registration services for the TLD must be able to automate these processes to at least some degree.

The GDPR specifically lifts the prohibition against automated individual decision-making for cases in which the controller has no decision-making power, namely whether or not to process personal data necessary to comply with a legal obligation under EU or EU Member State law to which the controller is subject (cf. Art. 22 (2) b GDPR). However, EU data protection law requires that the EU or EU Member State law provides for suitable measures to safeguard the data subject's rights and freedoms and legitimate interests (cf. Art. 22 (2) b GDPR). Such safeguarding measures are currently missing in the NIS 2 Directive and should be added along with an obligation for the Member States to ensure that TLD registries

and the entities providing domain name registration services for the TLD are able to automate these processes to at least some degree.

c. Completeness and Accuracy of Domain Name Registration Data

Art. 23 (1) NIS 2 Directive requires Member States to ensure that TLD registries and the entities providing domain name registration services for the TLD collect and maintain accurate and complete domain name registration data in a "dedicated database facility with due diligence" subject to EU data protection law, with respect to data that are personal data. According to Recital 61 of the NIS 2 Directive, TLD registries and the entities providing domain name registration services for the TLD shall even "*guarantee"* the integrity and availability of domain name registration data.

No body or company, including TLD registries and the entities providing domain name registration services for the TLD, can *guarantee* the integrity and availability of domain name registration data. However, TLD registries and the entities providing domain name registration services for the TLD are required under the GDPR (and, for entities providing gTLD domain name registration services pursuant to agreements with ICANN) to implement technical and organizational measures appropriate to the risk to safeguard the integrity and availability of domain name registration data that they receive. Therefore, ICANN org suggests to delete "*and guarantee the integrity and availability of*" in Recital 61. Within the scope of applicability of the GDPR, the requirement to implement appropriate technical and organizational measures for the security of personal data already applies irrespectively to TLD registries and the entities providing domain name registration services for the TLD, pursuant to Art. 32 GDPR.

Furthermore, requiring TLD registries and the entities providing domain name registration services for the TLD to collect and maintain data "in a dedicated database facility" does not necessarily foster the integrity and availability of domain name registration data. Limiting storage to a dedicated database facility may even be counterproductive to the integrity and availability of domain name registration data, as any interference with such dedicated database facility would endanger the integrity and availability of all domain name registration data. This requirement might also be understood as permitting only storage in an "on premise" database facility, but not in a cloud-based database. Again, with respect to registration data containing personal data, TLD registries and the entities providing domain name registration services for the TLD are already required to implement technical and organizational measures appropriate to the risk to safeguard the integrity and availability of domain name registration data under the GDPR. With regard to the ongoing technical development, they should be left with discretion to determine the appropriate technical and organizational means to ensure the integrity and availability of domain name registration data.

As a further point, it is unclear to what the addition to collect and maintain domain name registration data "*with due diligence subject to Union data protection law as regards data which are personal data*" relates. This could be read to apply to either the accuracy

principle or the storage in a dedicated database facility. The addition seems to be unnecessary and misleading. TLD registries and the entities providing domain name registration services for the TLD which process personal data subject to the GDPR have to comply with the relevant GDPR provisions irrespective of this addition. However, by referring to EU data protection law such addition creates uncertainties regarding the scope of the accuracy principle under Art. 23 (1) NIS 2 Directive, in particular whether the accuracy principle stipulated in Art. 23 (1) NIS 2 Directive only relates to personal data or to all domain name registration data. ICANN org would assume that all domain name registration data shall be accurate.

Therefore, ICANN org suggests to delete "*in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data"* in Art. 23 (1) and Recital 61 of the NIS 2 Directive.

In addition, ICANN org suggests that the NIS 2 Directive should specify or require EU Member States to specify minimum data categories for domain name registration data to be considered complete to avoid any conflict with the data minimization principle under the GDPR, which could require TLD registries and the entities providing domain name registration services for the TLD not to collect and maintain certain data categories which may, however, be required by legitimate access seekers for their lawful request.

ICANN org would suggest that complete domain name registration data could include the following data categories, as identified by the ICANN community's Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data's Phase 1 Final Report,[5] at recommendation 5:

- Domain Name
- Registrar Registration Data (WHOIS) Server
- Registrar URL
- Registrar Registration Expiration Date
- Registrar
- Registrar IANA ID
- Registrar Abuse Contact Email
- Registrar Abuse Contact Phone
- Reseller (where applicable)
- Domain Status(es)
- Registrant Name
- Registrant Organization (where applicable)
- Registrant Postal Address
- Registrant Country
- Registrant Phone
- Registrant Email

[5] See EPDP Phase 1 Final Report at https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf.

d. Acknowledging a Reliable, Resilient and Secure Domain Name System as an Important Public Interest

In Recital 15, the NIS 2 Directive already acknowledges that 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.

The DNS is transnational, and the TLD registries and the entities providing domain name registration services for the TLD operate globally (cf. Recital 64 of the NIS 2 Directive), having to comply with requests from legitimate access seekers from different jurisdictions in the world.

In this regard ICANN org has already addressed its concerns regarding the strict requirements for international data transfers stipulated by the European Data Protection Board (EDPB) in its "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" following the invalidation of the EU-US Privacy Shield in the *Schrems II* decision of the Court of Justice of the EU (CJEU). These concerns are particularly critical with regard to the Use Cases 6 (Transfer to cloud services providers or other processors which require access to data in the clear) and 7 (Remote access to data for business purposes), for which the EDPB has determined that no effective supplementary technical measures could be found to ensure an essentially equivalent level of protection for the data transferred to a third country.

To enable TLD registries and the entities providing domain name registration services for the TLD to uphold and preserve a reliable, resilient, and secure domain name system (DNS), TLD registries and the entities providing domain name registration services for the TLD must be able to transfer registration data, which may or may not include personal data, internationally. To this end, specifically acknowledging the importance of upholding and preserving a reliable, resilient, and secure DNS as an important public interest would enable TLD registries and the entities providing domain name registration services for the TLD to transfer personal data internationally, if the requirements of Art. 49 (1) d GDPR are met, thereby paving a way for the necessary international operation of the DNS in the aftermath of the *Schrems II* ruling.

e. Defining Unspecified Terms

Art. 23 NIS 2 Directive contains many undefined and unspecified terms. To ensure a proper and streamlined application within the EU, the NIS 2 Directive should clarify at least the following terms:

- Art. 23 (1) NIS 2 Directive requires to collect "*complete domain name registration data.*" According to Art. 23 (2) NIS 2 Directive EU Member

States shall ensure that registration data includes "*relevant information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs."*

As mentioned in the foregoing point c, ICANN org suggests that the NIS 2 Directive should specify minimum categories for the domain name registration data to be considered complete in terms of the NIS2 Directive.[6]

Clarification of minimum data categories, for example in Recital 62, would help to streamline application across the EU, thereby making access to domain name registration data more efficient, and prevent any misunderstanding and dispute when having to weigh the completeness of domain name registration data against the data minimization principle under the GDPR.

- Art. 23 (4) NIS 2 Directive requires to "*publish (...) domain registration data which are not personal data.*"

There is no clear-cut line between personal and non-personal data, even in connection with legal person names and domain names.[7] ICANN org therefore suggests specifically stipulating which data categories should be published following the registration of a domain name such as, for example, name and domain name of legal persons as well as the contact details. With regard to contact details, Art. 24 (4) NIS 2 Directive could include the exception that only the provision of non-personal contact details is required.

- Art. 23 (5) NIS 2 Directive requires *"TLD registries and the entities providing domain name registration services for the TLD to provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law."*

It should be clarified to which data categories "specific" domain name registration data relates. A list of the minimum data categories to which access must be provided or examples of minimum requirements should be specified,

[6] Cf. Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive of the European Data Protection Supervisor, p. 12: "*The EDPS recommends clearly spelling out what constitutes "relevant information" for purposes of this provision, including personal data, taking into account the principles of necessity and proportionality. Doing so would promote legal certainty, as well as a ensuring a consistent approach across the EU's 27 Member States*."

[7] Cf. Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive of the European Data Protection Supervisor, p. 12 et seq.: "*The EDPS equally recommends clarifying in greater detail which categories of data domain registration data (which do not constitute personal data) should be the subject of publication.*"

for example, in Recital 62. This would also help to ensure compliance with regard to the data minimization principle under the GDPR.

ICANN org also suggests clarifying when a request can be considered "lawful and duly justified."[8] The clarification that compliance with the NIS 2 Directive and its implementing law is considered compliance with a legal obligation in terms of Art. 6 (1) c, and Art. 6(1)(3) GDPR would avoid any misunderstanding, which may affect the effectiveness of access to domain name registration data.

To ensure that access to personal data is not mistakenly provided to unqualified access seekers, the NIS 2 Directive should also specify which access seekers qualify as "legitimate" in terms of the NIS 2 Directive.[9]

f. Closing Remarks

The issues raised in this comment are critical to the work of ICANN org, the gTLD registries and registrars, and the DNS as a whole. We strongly encourage you to take these points into account, particularly concerning the NIS2 Directive's broad scope, and the need for added clarity in its Art. 23.

* * *

[8] Cf. Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive of the European Data Protection Supervisor, p. 13 et seq.: *"The Proposal neither defines what is to be understood by "lawful and duly justified requests", nor defines "legitimate access seekers", nor specifies any purposes for such access. The Proposal also does not lay down any objective criterion by which to determine the limits of the access of "legitimate access seekers" to the data and their subsequent use. (...) In the same vein, the EDPS also recommends introducing further clarification as to what constitutes a "lawful and duly justified" request on the basis of which access shall be granted, and under which conditions."*

[9] Cf. Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive of the European Data Protection Supervisor, p. 13 et seq.: *"The Proposal neither defines what is to be understood by "lawful and duly justified requests", nor defines "legitimate access seekers", nor specifies any purposes for such access. The Proposal also does not lay down any objective criterion by which to determine the limits of the access of "legitimate access seekers" to the data and their subsequent use. (...) the EDPS underlines that the text of the Proposal must therefore further clarify which (public or private) entities might constitute "legitimate access seekers"."*