

Interisle

Domain Name Contact Data Availability and Registrant Classification Study

A Study of the Effects of GDPR, ICANN Policy and Market
Forces, and the Potential Effects of NIS 2

Prepared for DNIB.com by

Greg Aaron, Lyman Chapin, David Piscitello, Dr. Colin Strutt

Interisle Consulting Group, LLC

4 June 2024

Table of Contents

Introduction and Purpose	3
Findings	4
Legal and Policy Background	6
GDPR and Resulting ICANN Temporary Specification	6
Study Methodology	8
Sample Selection and Margin of Error	8
Contact Data Publication Category	10
Registrant Type Classification	12
GDPR Jurisdiction	15
Study Results	17
Contact Data Publication Category	17
Domain Registrant/User Type Classification	19
Use of Proxy/Privacy Services	22
Proxy-Protected Registrants	23
Reach of GDPR Based on Jurisdiction	24
GDPR Jurisdiction of Redacted Domains	26
Reach of GDPR Based on Jurisdiction <i>and</i> Legal Character	26
NIS 2: Implications for Contact Data Availability	29
Appendix A: TLD Representation in Sample Set	32
Appendix B: Registrar Representation in Sample Set	34
About Interisle Consulting Group, LLC	35
About the Authors	35

Introduction and Purpose

This study provides data about the current availability of domain name contact data in the generic top-level domains (gTLDs). It also compares the current state with past studies to document changes over time. This includes measurement of the combined effects of the European Union’s General Data Protection Regulation (GDPR) from its enactment in 2018 to the present, the effects of ICANN’s resulting policies, changes in registrar privacy offerings and registrant behavior, and the potential effects of the EU’s new NIS 2 Directive.

Domain names are one of the essential components of the Internet. These identifiers allow web sites, email, and apps to function. *Domain name registration data* includes the information about who registered and controls the domain name (“contact data”), and has historically been available for lookup via a “registration data directory service” (RDDS) system using the WHOIS¹ and RDAP² protocols. This data has served a variety of legitimate purposes, it: provides a way to get in touch with domain owners to solve problems, captures who has legal rights to the domain name, provides an additional data point for establishing trust online, and is useful data for fighting cybercrime. Domain name registration data has also, however, been misused to send spam, malware, and unsolicited offers, and been harvested and sold for commercial purposes. The GDPR introduced new requirements for safeguarding personal data. This created a tension between two goals: protecting personal data, while also continuing to make non-sensitive data available and therefore preserving the utility of the registration data system itself.

Specifically, this study:

- Determines how many gTLD domains have identifiable contact data available via RDDS, versus how many have contact data obscured by either proxy protection or redaction.
- Examines the legal character of registrants: how many are individuals or “natural persons” versus incorporated entities or “legal persons.”
- Examines the laws and ICANN policies that affect the availability of contact data and measures the effects over time and across jurisdictions.
- Notes differences in business practices/policy implementation among registrars.
- Explores how NIS 2 may affect the public availability of registration data in the near future.
- Note: This study does not consider the impact of privacy laws in countries outside the EEA. This is beyond the scope of this study.

Our findings are based on statistically valid samples. As such this data can be used as a basis for fact-based discussion and decision-making (see *Study Methodology*).

¹ RFC 3912: WHOIS Protocol Specification – <https://www.rfc-editor.org/rfc/rfc3912>

² RFC 7480: HTTP Usage in the Registration Data Access Protocol (RDAP) – <https://www.rfc-editor.org/rfc/rfc7480>

See also RFCs 7481, 8056, 9082, 9083, 9224, and gTLD RDAP profile: <https://www.icann.org/gtld-rdap-profile>

Findings

The major findings of this study are:

1. Only 10.8% of gTLD domains have identifying contact data for the actual domain name registrant available via RDDS. Before the GDPR went into effect in mid-2018 and ICANN changed its registration data policy in response, the actual identities of about 75.7% of gTLD domain name registrants were available in RDDS. *(Page 17)*
2. For almost two-thirds of gTLD names – 65.7% – the actual domain name registrant or beneficial user cannot be identified either via RDDS or by examining the domains' web site content. Before mid-2018, only 18% of domain users could not be identified. By our 2021 study, 51.7% were unidentifiable. The change from 2021 to 2024 is due to the increased use of proxy protection. *(Pages 8, 24)*
3. The use of proxy protection has increased significantly in the last three years. Currently, 58.2% of all gTLD domains are proxy-protected, up from 29.2% in 2020 and 20.1% in 2013. *(Page 17)*
4. In 2020, registrars and registry redacted contact data from 57.3% of all gTLD domains. By early 2024, the percentage of domains with redacted contact data has fallen to 29.9%, as registrars shifted to proxy protection. *(Page 15)*
5. Since 2020, most of the largest registrars have made proxy protection a standard feature for almost all newly registered and many existing domains. Proxy services today are generally owned by the associated registrars, and the use of unaffiliated, third-party proxy services is negligible. *(Page 19)*
6. We estimate that at least 23.3% of gTLD domains are currently covered by the GDPR's jurisdictional reach. This is virtually the same as in 2020. These are the domains for which the registrant, registrar, registry operator, or registry back-end provider is located in the EEA. *(Page 24)*
7. While this estimated 23.3% of all domains falls within the GDPR's jurisdictional reach, only 12.5% of domains had a registrant that resided in the EEA. By protecting personal data *processed within* the EU, the GDPR's reach extends protection beyond EU residents to a larger set of domains and registrants. *(Page 26)*
8. The study data suggest that only around 11.6% of domains may belong to natural persons who are subject to GDPR. This is the percentage of domains that is *necessary to protect* under GDPR. In contrast, 89.2% of domains have either proxy-protected or redacted contact data. *(Page 24)*
9. Different registrars have made very different choices about what and how much contact data they redact or place under proxy protection, even when the registrars face similar jurisdictional and business situations. Significant differences exist in the display of contact data for registrants outside of GDPR's jurisdictional reach. *(Page 17)*
10. The data indicates that domain name registrars have significant control over (or have effective influence on) whether their registrants' contact data is displayed in RDDS. It appears that registrants rarely opt into publication of their data in RDDS. *(Pages 19 and 23)*

11. NIS 2 includes provisions that should increase the publication of contact data in RDDs, specifically that of legal persons. Depending on EU Member State legislative implementation, NIS 2 could boost identifiable contact data availability from 10.8% of all gTLD domains to as much as 22.5%. The results may depend significantly on each EU Member State's resulting legislation and on registrars' and registry operators' implementations. *(Page 29)*

Legal and Policy Background

This section describes *why* domain registration data availability has changed over the last six years, *what* data is affected, and *how* data must be handled now and in the immediate future.

GDPR and Resulting ICANN Temporary Specification

The Internet Corporation for Assigned Names and Numbers (ICANN) has oversight over the generic top-level domains (gTLDs), such as .COM, .ORG, and .ONLINE. ICANN decides what parties manage gTLD registries, accredits registrars and licenses them to sell gTLD domains, maintains binding contracts with its registry operators and registrars, and has mechanisms for making new policies through a multi-stakeholder process. ICANN policy does not apply to country-code domains (ccTLDs); ccTLDs are beyond the scope of this study.

The General Data Protection Regulation (GDPR) was adopted by the European Union (EU) and took full effect on 25 May 2018. This important data protection and privacy law had a significant impact on how domain name registration data could be made available.

Before GDPR, ICANN policy and contracts required that domain name contact information be made available via the WHOIS system, allowing anyone to look up the name and contact data of domain registrants and their administrative and technical contacts. But the GDPR restricted the publication of personally identifiable data belonging to natural persons located in the EU, and the data of any natural person whose data is processed within the EU. (A *natural person* is a human being. In contrast, a *legal person* is a non-human entity incorporated under the law of its jurisdiction, such as a company.)

In response, the ICANN Board of Directors established the *Temporary Specification for gTLD Registration Data*³, effective on 25 May 2018. This Temporary Specification was affirmed in May 2019 under *the Interim Registration Data Policy for gTLDs*⁴. In this policy, ICANN requires that registrars and registry operators protect personal data covered under the GDPR. The policy was made permanent, with minor modifications, in 2024.⁵

Notably this policy also allows registrars and registry operators to redact (withhold details from RDDS) the data of any domain contacts, including contact data that is *not* protected by GDPR or a similar data protection law. This created a tension between the two stated goals: protecting data that must be

³ <https://www.icann.org/resources/pages/gtld-registration-data-specs-en/#temp-spec>

⁴ <https://www.icann.org/resources/pages/interim-registration-data-policy-en>

⁵ Registration Data Policy: <https://www.icann.org/resources/pages/registration-data-policy-2024-02-21-en>

Contracted parties may implement this Policy beginning on 21 August 2024 and must implement no later than 21 August 2025.

protected by law, but also continuing to make data available (and therefore preserving the utility of the WHOIS system itself) “to the greatest extent possible.”⁶

⁶ Blog by ICANN CEO Göran Marby, <https://www.icann.org/news/blog/data-protection-privacy-issues-update-an-icann-update-most-frequently-asked-questions>. In the *Temporary Specification*, this goal is stated as: “consistent with ICANN's stated objective to comply with the GDPR, while maintaining the existing WHOIS system to the greatest extent possible.”

Study Methodology

Our study methodology takes the above legal and policy requirements into consideration.

To the extent possible, this study and our 2021 study used methodologies established in previous studies that were commissioned by ICANN. The methodologies provide objective and statistically valid results, provide continuity, and allow for comparisons over time. Those key studies were:

- “WHOIS Registrant Identification Study”⁷ of 2013, and its accompanying “Terms of Reference for WHOIS Registrant Identification Studies”⁸ methodology document. These were designed and executed for ICANN by NORC at the University of Chicago, an independent, non-partisan research institution. They provide methodologies for establishing whether a domain is sponsored by a natural or a legal person, what a privacy/proxy registration is, establishing the percentage of privacy/proxy use among legal persons, and so on.
- Entity classification and privacy/proxy service identification methodologies developed in:
 - The “Study of the Accuracy of WHOIS Registrant Contact Information”⁹, developed for ICANN by NORC at the University of Chicago in 2010.
 - “ICANN Study on the Prevalence of Domain Names Registered using a Privacy or Proxy Service among the top 5 gTLDs”¹⁰, conducted by ICANN Organization in 2010.
 - The “WHOIS Privacy and Proxy Abuse Study”¹¹ and its terms of reference¹² document, developed for ICANN by the National Physical Laboratory of the U.K. in 2014.
 - The “WHOIS Proxy/Privacy Reveal & Relay Feasibility Survey”¹³, developed for ICANN by Interisle Consulting in 2012.

Sample Selection and Margin of Error

In December 2023 we downloaded and collated the October 2023 ICANN registry reports for all gTLDs, which were the latest available at that time.¹⁴ This allowed us to determine the size of the gTLD namespace (a population size of 219,258,959 domains total), the size of every gTLD, and how many domains were sponsored by each registrar.

⁷ https://gns0.icann.org/sites/default/files/filefield_39861/registrant-identification-summary-23may13-en.pdf

⁸ https://gns0.icann.org/sites/default/files/filefield_24703/tor-whois-registrant-id-studies-20may11-en.pdf

⁹ <https://www.icann.org/en/system/files/newsletters/whois-accuracy-study-17jan10-en.pdf>

¹⁰ <https://www.icann.org/en/system/files/newsletters/privacy-proxy-registration-services-study-14sep10-en.pdf>

¹¹ <http://whois.icann.org/sites/default/files/files/pp-abuse-study-final-07mar14-en.pdf>

¹² https://gns0.icann.org/sites/default/files/filefield_12392/whois-proxy-abuse-study-18may10-en.pdf

¹³ https://gns0.icann.org/sites/default/files/filefield_35963/whois-pp-survey-final-report-22aug12-en.pdf

¹⁴ Monthly registry reports: <https://www.icann.org/resources/pages/registry-reports>

For the current study, and consistent with our 2021 study, we created a study set of 3,000 domains. (NORC's "Registrant Identification Study" of 2013 only used a data set of 1,600 domains.¹⁵) Our larger set provides a 98% confidence level with a margin of error of $\pm 2\%$. It also allows a proportional estimate's margin of error at the 95% confidence level of $\pm 5\%$ for any subgroup with 400 or more domains. Our larger set also allowed us to include new top-level domains to represent the expanded namespace.

Following the NORC methodology, we determined how many domains from the study set would be drawn from each gTLD, to reflect their share of the gTLD namespace. Our study set contains domains from the 20 largest gTLDs, plus an additional five chosen from the next-largest new gTLDs. The details are presented in *Appendix A: TLD Representation in Sample Set*.

- The 25 TLDs contain 207.2 million domains, or 95% of all registered gTLD domains. The selection pool was therefore representative of the gTLD space.
- The selection of TLDs ensured that the study set contains gTLDs administered by each of the major registry operators, and at least two TLDs serviced by each of the major back-end providers. This allows the study set to contain domains administered in different geographic regions, including some located in the European Union and therefore subject to GDPR. The selection is also useful because different registrars, registry operators, and back-end providers make different choices about how to serve WHOIS data.
- The new gTLDs represent about 14.5% of the gTLD market (31.8 million out of 219.3 million domains). To allow the study of new gTLDs, they are slightly over-represented in our study set, which contains 475 new gTLD domains, or 15.8% of the study set. The .COM domain was therefore slightly under-sampled in comparison to its market share but a similar under-sampling of .COM was also done in the NORC study.
- Each gTLD had at least 20 domains in the study set. A larger number was not necessary because this study does not seek to make detailed comparisons across gTLDs.

We then obtained the zone files for the 25 gTLDs in early January 2024, and randomly selected the requisite number of domains from each gTLD's zone file. The randomness was obtained by using the PHP library routine `mt_rand`¹⁶, which generates a random value via the Mersenne Twister Random Number Generator.¹⁷

We then obtained data for the 3,000 domains from each registry's port 43 WHOIS server. This told us which registrar sponsored each domain. We next queried each registrar's port 43 WHOIS server for its domains. (Domain contact data for .COM and .NET domains is exclusively held at the registrars.)

¹⁵ NORC's "Registrant Identification Study" of 2013 WHOIS used a data set of 1,600 domains, designed to provide a margin of error at the 95% confidence level of $\pm 5\%$. The NORC study used domains from only five top-level domains (.COM, .NET, .ORG, .INFO, and .BIZ) and was conducted before a thousand-plus new generic top-level domains were introduced by ICANN beginning in late 2013.

¹⁶ [PHP: mt_rand](#)

¹⁷ [Mersenne Twister: A random number generator](#)

We then evaluated the study set to see if it reasonably reflected gTLD market share by registrar. When randomly drawing 3,000 domains from the pool of 207.2 million, there can be “draws” that are statistically anomalous. For example, it is possible (but statistically unlikely) to perform a draw in which none of the selected 3,000 domains are sponsored by GoDaddy, which owns 28.7% of the gTLD market. We determined that the registrars’ proportions of our “draw” reasonably tracked their proportions of market share. There were only three large registrars whose percentage representation in the study set varied from their market share by 0.5% or more. We were therefore satisfied that the randomly selected study set adequately reflects registrar gTLD market share, and again is representative of the gTLD space as whole. For details, please see *Appendix B: Registrar Representation in Sample Set*.

We collected domain name registration data immediately after we performed the random selection. We began visiting web sites in late January 2024 and continued into early February 2024. Only a handful of domain names expired after the registration data was collected but before we performed site visits. We compensated for those cases by referring to snapshots of those sites at the Internet Archive.

The collected registration data was parsed and, where necessary, manually processed to prepare the data for analysis. There were numerous cases in which registrars withheld all contact data fields from their port 43 output,¹⁸ but we were able to gather it by hand using the registrars’ web based WHOIS services. Some registrars failed to provide any registration data – none via their port 43 servers, nor on their web-based WHOIS lookup pages, nor via RDAP. For these 36 domains, we counted the contact data as redacted.

We made use of web browsers, the curl command-line utility, file security addons ([OPSWAT](#), [Google Safe Browsing](#)), and URL blocklist checkers ([Spamhaus](#), [MXToolbox](#)) for our web site visits. These provided accurate DNS resolution data as well as HTTP and SSL (certificate) error [data](#).

Contact Data Publication Category

Contact data publication category describes what *kind and amount of contact data* is published in RDDS for a given domain name. In earlier studies, domains only fell into two categories: full contact publication available in RDDS, or privacy/proxy. However, developments since 2018 required us to create a third category: contact data redacted. The publication category a domain is placed in reflects choices made by the registrant and/or its registrar. The three categories are:

- 1. Contact data available:** Contact data for the domain registrant is available in RDDS and is not privacy/proxy data. The name of the registrant is provided, and there is street address data (and usually phone and email address) data present.
- 2. Privacy/Proxy:**
 - *Privacy services* offer alternate RDDS contact information and mail forwarding services, but do not shield the Registered Name Holder’s identity. Domain records under privacy

¹⁸ Some registrars withheld contractually required fields such as Registrant Country.

protection therefore feature the registrant's real name and address information is present in the domain record.

- *Proxy services* register domain names on a third party's behalf and then license their use so that the provider's identity and contact information (and not the licensee's) is published in RDDS. With proxy services, the identity of the "real" registrant is not revealed.
- Per ICANN policy, the name and the full contact data of a privacy/proxy service provider must be published in RDDS, including the provider's name, street address, and telephone number. This allows domains under proxy protection to be identified reliably.
- In the past, obtaining the actual domain user's name from RDDS during any study was likely for Privacy registrations, but not for domains registered by a Proxy provider.¹⁹ However, it is now more difficult to identify Privacy registrations as many now appear to be obscured by the application of either redaction or proxy privacy.

3. Contact data redacted: Contact data is redacted (withheld) from publication in RDDS, as allowed by ICANN's *Temporary Specification*²⁰ and *Interim Registration Data Policy for gTLDs*²¹. Under those policies, since May 2018, gTLD registrars and registry operators are required to redact personally identifiable data (the contact's name, street address, phone number, and email address) from contact data IF:

- the registrant is in the European Economic Area (EEA), or
- the registrar or registry operator is in the EEA, or
- the registrar or registry operator is outside the EEA but processes the data within the EEA. This occurs when a registry operator uses a back-end service provider located in the EEA.

Note that:

- gTLD registrars and registry operators are *allowed* for commercial or technical reasons to redact personal data for any other domains, including those not covered by GDPR or any other privacy law.
- Per the policies above, registrars and registry operators who redact data from a domain record must either publish text in the redacted contact data fields substantially similar to "REDACTED FOR PRIVACY", may provide no information in the value section of the redacted field, or may not publish the redacted field at all. Therefore, domains with redacted data can be clearly distinguished from domains in the "Contact Data Available" and "Privacy/Proxy" categories.
- The fields that can be redacted include Registrant Name, the Street Address and Postal Code fields, and Telephone Number. ICANN policy requires that the State and Country fields and the data in them must *always* be published in RDDS, because that data is not personally identifiable.

¹⁹ Definitions from revised "Terms of Reference for WHOIS Registrant Identification Studies", https://gnso.icann.org/sites/default/files/filefield_24703/tor-whois-registrant-id-studies-20may11-en.pdf

²⁰ See Appendix A, at <https://www.icann.org/resources/pages/gtld-registration-data-specs-en/#5>

²¹ <https://www.icann.org/resources/pages/interim-registration-data-policy-en>

- Some registrars redact Registrant Name and other fields but show data in the Registrant Organization field if the registrant supplied it.

Registrant Type Classification

We performed analysis to assign each domain's registrant into one of three registrant types: natural person, legal person, and unclassified.

The natural and legal person categories have legal significance under GDPR, NIS 2, and ICANN policy.

Our study *reliably establishes a minimum or floor for the percentage of domains that are registered by/used by legal persons, and by natural persons/users.* Below we describe our classification methodology, and why it is judicious.

Domain name registration data is the authoritative record of what party is the *registrant* of record, also known as the "registered domain holder." Some registrants are clearly identified via RDDS, and that data can be used to classify their registrant type. However, most of our classification work consisted of visiting each domain to see if it has a web site, and if so whether the web site reveals the identity (and thus type) of the user. While a domain can be privacy/proxy protected, or can have its contact data redacted, the domain's web site can reveal the domain user's identity. All 3,000 domains were visited.

In its 2013 study, NORC used WHOIS data to classify registrants into similar types. NORC examined the WHOIS data to assign each registrant an Apparent Registrant Type. NORC then examined the web sites on the domains to assign each domain to an Apparent Domain User Type. The "domain user" is the beneficial user of a domain name and is the party that makes use of the web site and evidently controls it. For example, the International Committee of the Red Cross is the domain user of ICRC.ORG, as is evident from the web site.

But in most cases, NORC found that the registrant of record and the site user were one and the same. This is logical and unsurprising. NORC found that *"there is a strong relationship between apparent registrant type and apparent domain user type, with a p-value for the relationship of less than .0001."*

The registrant of record and the domain user can technically be different, but for the purposes of this study the difference may not matter when determining registrant type. For example, Company X may hire a web design firm to create a web site for it. Sometimes Company X may be listed as the registrant in WHOIS and is the user of its domain too. Sometimes the web design firm may list itself as the registrant, and Company X is the site user.

However, both parties are companies (*i.e.*, legal persons), and so the difference does not matter when assigning registrant type. Also, Apparent Registrant Type is no longer useful to break out as a separate category for analysis, because after mid-2018 identifying contact data was available for only a small percentage of gTLD domain names.

A *natural person* is a human being. In contrast, a *legal person* is a legal entity incorporated under the law of a jurisdiction. The distinction is important for ICANN policy, which was designed to allow compliance with GDPR. GDPR only protects the data of natural persons. The text of the GDPR says:

The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.

*This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.*²²

NIS 2 goes further, and requires that registries and registrars publish the data of legal persons in RDDs:

*Member States shall require the TLD name registries and the entities providing domain name registration services to make publicly available, without undue delay after the registration of a domain name, the domain name registration data which are not personal data.*²³

*TLD name registries and entities providing domain name registration services should be required to make publicly available domain name registration data that fall outside the scope of Union data protection law, such as data that concern legal persons... For legal persons, the TLD name registries and the entities providing domain name registration services [registrar and resellers] should make publicly available at least the name of the registrant and the contact telephone number. The contact email address should also be published, provided that it does not contain any personal data, such as in the case of email aliases or functional accounts.... Member States should ensure that all types of access to personal and non-personal domain name registration data are free of charge.*²⁴

Accordingly, we coded the domain user as a *legal person* if one of these cases applied:

- The entity identified itself as a company in RDDs data and/or on its web site. In most cases the entity did so with a specific legal form (*Inc., LLC, Limited, Pty, LLP, etc.*), or displayed a business registration number. In some cases, the exact legal character or exact legal form of an entity was not mentioned in RDDs data or on the web site, but we were able to confirm incorporation via a reputable database (such as Dun & Bradstreet, the U.K.'s Companies House, or a Secretary of State database), from the domain's historical data, or from the entity's own social media accounts, linked to from its web site.
- The entity is an incorporated not-for-profit entity. For example, we encountered U.S. 401(c)3 entities, registered trusts and charities, and a Kenyan Community-Based Organization (CBO) – a

²² GDPR Recital 14. <https://gdpr.eu/recital-14-not-applicable-to-legal-persons/>

²³ NIS 2 Article 28, Database of domain name registration data, paragraph 4. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555&qid=1709146869690#d1e3770-80-1>

²⁴ NIS 2 Recital 112. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32022L2555>

legal form that requires government registration. The site Charity Navigator²⁵ provided confirmation of many U.S. 501(c)(3) organizations in the United States.

- The entity is a government (local, state, or national). This includes public schools.
- We did not use commercial activity as a decisive classification criterion. Whether a legal entity is for-profit or not-for-profit, or whether a natural person or legal person is engaged in commercial activity, does not matter for the purposes of the GDPR, NIS 2, or ICANN policy.

We coded the domain user as a *natural person* if:

- The web site was devoted to personal endeavors – for example blogs, wedding sites, hobbies, etc. – or,
- The party was an unincorporated sole proprietor.

We coded the domain user as *unclassified* if:

- We could not satisfactorily establish the identity of the registrant or user. In most of these cases there was no real registrant data to rely upon, and the web site did not feature any content that could be evaluated.
- We were unable to establish the exact legal character of the registrant. For example, we encountered sites engaged in business activity, but we could not determine whether the registrant/user is incorporated or not. This was the case with some individuals engaged in professional activities – for example photographers using their sites to display their professional portfolios, yoga instructors, etc. – who might be incorporated or might be sole proprietors.

We did not code domains as belonging to a natural person based *solely* on WHOIS data. This is because we found examples where the Registrant Name and/or Registrant Organization fields list only the name of a natural person, but the site is clearly operated by or dedicated to a legal person. In some such cases we established that the listed natural person was an employee of the legal person site user. Some of these are cases in which the registrant probably should have listed the legal organization as the Registrant but did not know to do so. Also, some registrars decline to publish the Registrant Organization field or the data in it (a choice allowed by ICANN policy), and that removes a vital piece of data from consideration.

Following the methodology of the NORC study, we documented rules to be uniformly applied during the site visits, and independently classified some of the same sites and then compared the results to reconcile discrepancies and reinforce uniformity. We used [Google Translate](#) to examine sites in languages other than English. When the analysts visited each domain, they made a note describing what they found.

Some legal person registrants include the contact data of natural persons in their domain name registration records. Unfortunately, it is no longer possible to determine how many legal person

²⁵ <https://www.charitynavigator.org/>

registrants put the contact data of natural persons in their domains name records, because so many records are now proxy-protected or redacted. Studying that issue would require a corpus of data obtained from registrars and is beyond the scope of this study.

Our methodology is conservative, allowing classification as a legal or natural person only when there is evidence. It acknowledges that many domains may be unclassifiable based on a lack of decisive, publicly available data. We followed the NORC study's principles: "registrant type was based on the evidence that we were able to discover during our investigation.... No attempt was made to verify WHOIS accuracy or contact the identified registrant."

GDPR Jurisdiction

To measure the effect of the GDPR and ICANN's data policy, we classified whether each domain's registration data is subject to GDPR based on whether any relevant party is within the jurisdiction of the EEA. The data is subject to GDPR if any of the following cases apply:²⁶

1. **The Registrant is located in the European Economic Area (EEA)**²⁷. We based this on the Registrant Country field in WHOIS, which is mandatory for registrars to publish.
2. **The domain's registrar or registry operator is established within the EEA.** We determined this by referring to ICANN's official lists.²⁸
3. **The domain's registrar and registry operator are established outside the EEA but processes the data within the EEA.** We therefore included registries that use a *back-end service provider* located in the EEA. A back-end provider provides infrastructure for the registry, including the registry system that processes and holds the domain data, and provides the WHOIS service. An example is back-end provider Team Internet (formerly called CentralNIC), which is in the United Kingdom and provides the infrastructure for the .XYZ registry operator of record, which is incorporated in the United States.²⁹

A few domains may have had resellers in the EEA, but the registrant, registrar, registry, and back-end provider were all outside the EU. The number of such domains is probably very small. This is not possible to measure because most registrars choose not to identify their resellers in WHOIS records.

²⁶ See ICANN Temporary Specification, Appendix A, section 2. <https://www.icann.org/resources/pages/gtld-registration-data-specs-en/#appendixA>

²⁷ The European Economic Area (EEA) consists of the Member States of the European Union (EU), plus three countries of the European Free Trade Association (EFTA): Iceland, Liechtenstein, and Norway. Although the United Kingdom has "Brexit" the European Union, we counted the U.K. as being under GDPR in our 2021 study because the U.K. followed GDPR in 2020. In the current study we continue to do so, because on January 1, 2021, the United Kingdom's UK GDPR rules became effective. The UK GDPR absorbs the privacy compliance requirements of the EEA's GDPR and combines them with the requirements of the U.K.'s Data Protection Act.

²⁸ <https://www.icann.org/en/accredited-registrars> and <https://www.iana.org/domains/root/db>

²⁹ <https://www.iana.org/domains/root/db/xyz.html>

Note: This study focuses on the reach of the GDPR, which is the major use case that affects the most domain names, and for which ICANN policy was largely developed to address. There may be jurisdictions outside the EEA that require similar protection of personal data in RDDs. Neither ICANN nor other parties have catalogued which jurisdictions those are. Evaluation of all the possibly relevant laws around the world is beyond the scope of this study.

Study Results

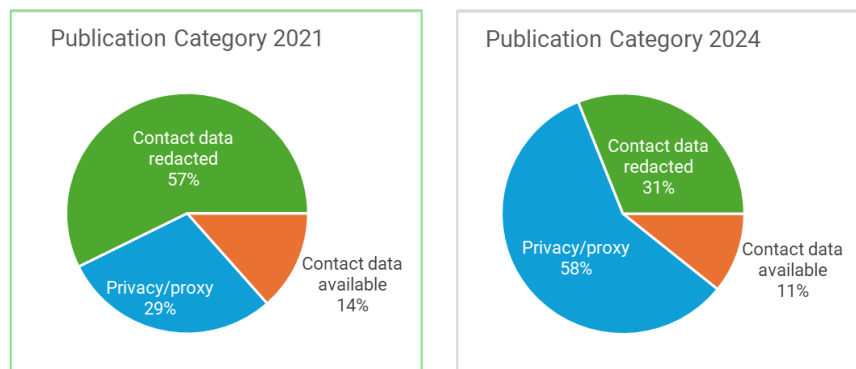
Contact Data Publication Category

In early 2018, prior to the adoption of EU GDPR and the associated ICANN domain registration policy, 75.7% of domain records in RDDS provided an identifiable registrant – a record that revealed the identity (including the name) of the registrant. The rest were privacy/proxy-protected. In our 2021 study, we determined that only 13.5% of domain records had an identifiable registrant. The other 86.4% of domain records had redacted contact data or were privacy/proxy-protected.

In early 2024, we observed that only 10.8% of domain records identified the actual registrant. Between 2021 and 2023, registrars shifted a large number of domains from redaction to proxy protection. Today:

- 58.2% of domain records (1,747 of 3,000) are now behind proxy-protection services.
- 31.0% of domain records (930 of 3,000) have redacted contact data. Of these 930 domains, 221 records revealed the Registrant Organization. These also reveal Registrant Country.

	2010 ³⁰	2013 ³¹	April 2018 ³²	November 2020	January 2024
Contact data available	82%	79.9%	75.7%	13.5%	10.8%
Privacy/proxy	18%	20.1%	24.3%	29.2%	58.2%
Contact data redacted	n/a	n/a	n/a	57.3%	31.0%



³⁰ Source: NORC, University of Chicago, “ICANN Study on the Prevalence of Domain Names Registered using a Privacy or Proxy Service among the top 5 gTLDs <https://www.icann.org/en/system/files/newsletters/privacy-proxy-registration-services-study-14sep10-en.pdf>

³¹ Source: NORC, University of Chicago, “WHOIS Registrant Identification Study”

³² This is Interisle’s calculation. In our 2021 study set of 3,000 domains, 1,420 had been registered before April 2018 (when registrars began preparing for the May 2018 GDPR deadline); 345 out of the 1,420 domains were proxy-protected. This calculation has a 95% confidence level and a margin of error of ±5%. The historical data was obtained from DomainTools.

Of the twenty largest registrars, only two make identifiable (non-proxy, non-redacted) contact data available in RDDS more than half the time:

Registrar	gTLD domains under management	Domains in study	Domains under proxy protection	Domains redacted	Domains contact data available	Contact data available %
GoDaddy.com	66,048,308	844	820	17	7	1%
Namecheap	16,138,187	229	205	10	14	6%
Tucows Domains	9,922,847	147	80	67	0	0%
Squarespace Domains II LLC	9,460,029	114	114	0	0	0%
GMO Internet Group d/b/a Onamae.com	5,001,879	87	64	6	17	20%
Network Solutions	5,126,007	67	28	12	27	40%
IONOS SE	4,734,076	64	33	31	0	0%
TurnCommerce DBA NameBright.com	4,888,575	63	1	1	61	97% ³³
Gname.com	4,285,751	61	0	61	0	0%
PDR d/b/a Public Domain Registry .com	4,431,131	58	15	11	22	40%
NameSilo	4,641,199	52	50	1	1	2%
eNom	3,963,106	52	10	42	0	0%
Dynadot	3,488,826	48	43	2	3	6%
Alibaba Cloud Computing d/b/a HiChina	3,219,314	44	42	2	0	0%
HOSTINGER	2,063,617	40	38	1	1	2%
Wix.com	2,768,148	40	0	29	11	28%
Alibaba Cloud Computing (Beijing)	2,677,411	32	0	32	0	0%
Wild West Domains	2,477,563	32	30	2	0	0%
Name.com	2,221,010	31	12	5	14	45%
CSC Corporate Domains	1,436,887	29	0	9	20	70%

³³ TurnCommerce DBA NameBright.com has a portfolio consisting almost entirely of domains owned by its partner HugeDomains.com. Both TurnCommerce and HugeDomains are located in the USA, and the portfolio is not subject to GDPR. HugeDomains primary business is the resale of domain names, and so perhaps making contact data available is an element of marketing those domain names.

The data indicates that registrars have significant control over how much contact data is available via RDDS, and what Contact Data Publication Category its registrants fall into. The numbers demonstrate that registrars are making very different choices as allowed by ICANN policy, even when they do business under similar circumstances.

For example, GoDaddy and Network Solutions are both headquartered in the U.S. They both have registrant bases that are U.S.-centric and mostly outside the EEA, and both companies cater to small-and-medium sized businesses. However:

- GoDaddy applied proxy protection to all its domain records (see “Use of Proxy/Privacy Services” below), and only 2% currently publish actual contact data.
- Network Solutions seems to redact data for its registrants in the EEA (both legal and natural persons) but publishes the contact data of many of its registrants outside the EEA.

In another example, Tucows and PDR are both based outside the EEA, both have reseller-oriented business models, and their registrants are mostly outside the EEA.

- Tucows put a blanket redaction strategy in place for GDPR but has been shifting to proxy-protection services. Currently, 46% of contact data at Tucows is redacted, and 54% is proxy-protected, leaving virtually no actual contact data publicly available.
- In contrast, PDR seems to redact all data for registrants in the EEA (both legal and natural persons) but publishes the contact data of registrants outside the EEA. In 2021, PDR published contact data for 62.5% of domains; currently PDR publishes contact data for 55% of its domains.

Some registrars in the Asia-Pacific region, notably Gname.com (100%), HiChina (98%) and Alibaba Cloud Computing Beijing (97%) also employ blanket redaction.

Registrars may use redaction and proxy protection for different reasons, and the two options have both common and unique effects on contact data. The common effect is that both take contact data out of the public realm. A unique effect of redacted domain records is that they will still show the Registrant Country, whereas proxy-protected domains will show the country of the proxy provider instead. This makes it more difficult to tell whether registrants are subject to GDPR or any similar privacy laws of other jurisdictions.

Domain Registrant/User Type Classification

We attempted to visit web sites for the 3,000 domains in the study set, using web browsers.³⁴ We also examined the contact data that was available via RDDS.

³⁴ We also used the [curl utility](#) to observe HTML protocol exchanges, which are helpful for identifying redirection, connection errors, and reachability issues. Prior to attempting connections, we used blocklist data from the [Cybercrime Information Center](#), [MXToolbox](#), or the [Spamhaus IP and Domain Reputation Checker](#) to determine whether the domain name or IP addresses where the domain name was hosted were safe to visit.

- 31.1% of domains were attributed to legal persons. (932 out of 3,000.)
- 4.2% of domains were attributed to natural persons. (126 out of 3,000.)
- The remaining 65.7% could not be classified as either legal or natural persons. (1,972 out of 3,000)
In these cases, the registrant/user was unidentifiable, or the registrant/user was identifiable, but their legal/natural status could not be determined.

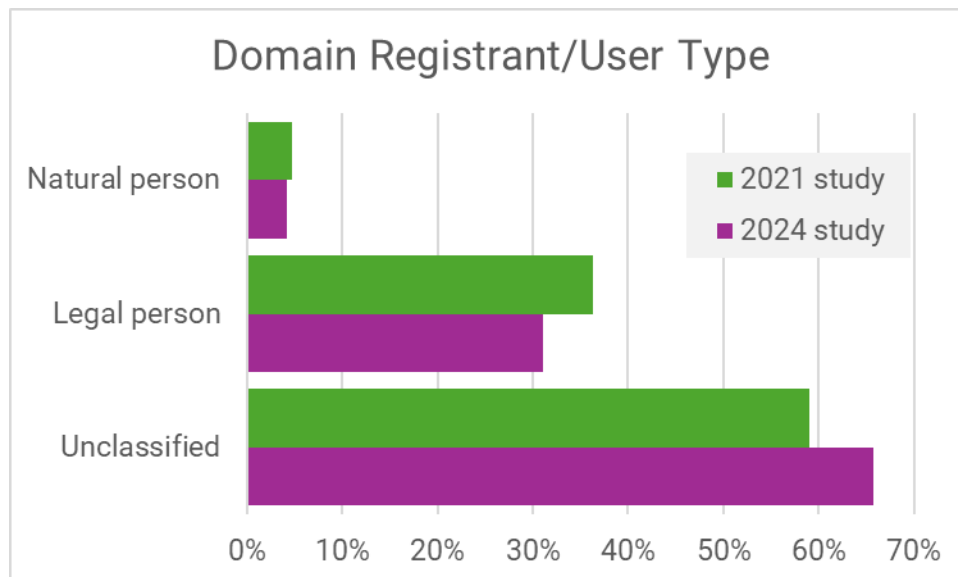
When we compare studies over time, we see a decline in the ability to classify domain user type:

Domain User Type	2013 (NORC)	2021 (Interisle)	2024 (Interisle)
Legal person	36.6%	36.3%	31.1%
Natural person	5.4%	4.7%	4.2%
Unclassified	56.0%	59.0%	65.7%

This recent decline is due to the overall decrease in availability of contact data. Otherwise, the legal/natural split has been consistent over the past ten years. **It has been consistently true that among attributable domains, legal persons have accounted for about seven times as many domains as natural persons.**

Note that the above reliably establishes a *minimum or floor* for the percentage of domains that are registered by/used by legal persons, and by natural persons/users.

In the study set of 3,000 domains, 1,972 domains (65.7%) were unclassifiable:



Two-thirds of gTLD domains could not be classified and attributed to a registrant user, either via domain registration data or by inspection of web site content. That is a significant shift from 2018,

before GDPR and ICANN’s Temporary Specification went into effect, when only 18% of domain registrants/users could not be classified.³⁵

The number of unidentifiable registrants/users is large because their registrant data was under proxy protection or was redacted, the domain had no web site content to evaluate, or the domain’s web site did not publish content revealing the registrant’s identity or legal character.

Attempts to access the web sites of 1,932 domains did not provide enough information to allow us to identify the registrant or classify the domain. The domains with unclassifiable natural person/legal person type included:

Type of non-identifying site	Number	% (of 3,000)
Parking pages	555	18.5%
Did not resolve (NXDOMAIN)	423	14.1%
Web site unreachable due to error (HTML error codes 4xx, certificate errors, etc.)	290	9.7%
Original content, but legal character could not be determined	268	8.9%
“Under construction” pages	183	6.1%
“Domain for sale” pages ³⁶	139	4.6%
Blank pages	42	1.4%
Had malware or phishing; some were flagged with interstitial warning pages.	24	0.8%
Access blocked due to Chinese national law	5	0.2%
“WHOIS verification pending” pages placed by registrars.	3	0.1%

³⁵ See “Contact Data Publication Category” above. Pre-GDPR, unidentifiable registrants were those that held privacy/proxy-protected domains (about 25% of all domains) minus those privacy/proxy domain holders who identified themselves in web site content. According to our current analysis, about 28% of privacy-proxy registrants identify themselves on their web sites. Assuming that registrants have not changed their general web presence practices over the past few years, this means that about 18% of domains were unidentifiable before GDPR and ICANN’s Temporary Specification went into effect.

³⁶ These “for sale” pages did not identify the ultimate registrant/seller and were usually provided by registrars and auction providers. Other “for sale” pages identified the owner as a domaining company, and so those were counted as owned by legal persons.

Use of Proxy/Privacy Services

The use of privacy/proxy services rose slightly after the GDPR and ICANN's Temporary Specification went into effect – from 24.3% in early 2018 to 29.2% in our 2021 study. **By early 2024, proxy services were used for 58.2% of domains.** (1,746 out of 3,000.) **This significant jump happened because many registrars decided to apply free, default proxy protection to most or all of the domains under their management.**

- The most prominent example was GoDaddy, the world's largest registrar. In June 2020, GoDaddy applied free proxy protection to all domains under its management.³⁷ Since then, GoDaddy has automatically applied free proxy protection to all new registrations and in-bound transfers.³⁸ GoDaddy allows its customers to opt into contact data publication, however most registrants have not used it.
- NameCheap, the industry's second-largest registrar, began giving away its WhoisGuard proxy service for free in May 2018, the month that GDPR went into effect.³⁹
- Google Domains⁴⁰ applied free proxy protection (provided by Tucows) automatically to all gTLD registrations. Google sold the registrar business to Squarespace in 2023, which continues to include proxy protection automatically.⁴¹
- Top-twenty registrars Tucows, NameSilo⁴², 1&1 IONOS SE⁴³, and Dynadot⁴⁴, among others, also give away proxy protection for free, usually as the default at registration.

Several of the industry's largest registrars now have proxy protection on the majority of the gTLD domains they sponsor. Examples from the data set include:

- NameCheap, Inc.: 86.8% proxy-protected (132 out of 152 domains).
- NameSilo: 97.1% proxy-protected (34 out of 35 domains).
- GMO Internet Inc.: 69.4% proxy-protected (59 out of 85 domains).

Nearly all the protected domains we identified were under *proxy* services. We were unable to clearly identify more than a handful of *privacy*-protected domains, where the registrant's real name was identified in the contact data. As noted earlier, some formerly privacy-protected domains have likely been

³⁷ <https://domainnamewire.com/2020/06/08/big-news-godaddy-starts-redacting-whois-information/>

³⁸ <https://www.godaddy.com/help/what-is-domain-protection-32311> Registrants can opt out of proxy protection.

³⁹ <https://www.namecheap.com/blog/free-whoisguard-forever/>

⁴⁰ <https://support.google.com/domains/answer/3251242?hl=en>

⁴¹ <https://support.squarespace.com/hc/en-us/articles/205812438-Whois-privacy>

⁴² <https://www.namesilo.com/Support/WHOIS-Privacy>

⁴³ <https://www.ionos.com/help/domains/preventing-spam-with-private-domain-registration/enabling-private-registration-for-a-11-ionos-domain/>

⁴⁴ <https://www.dynadot.com/domain/privacy.html>

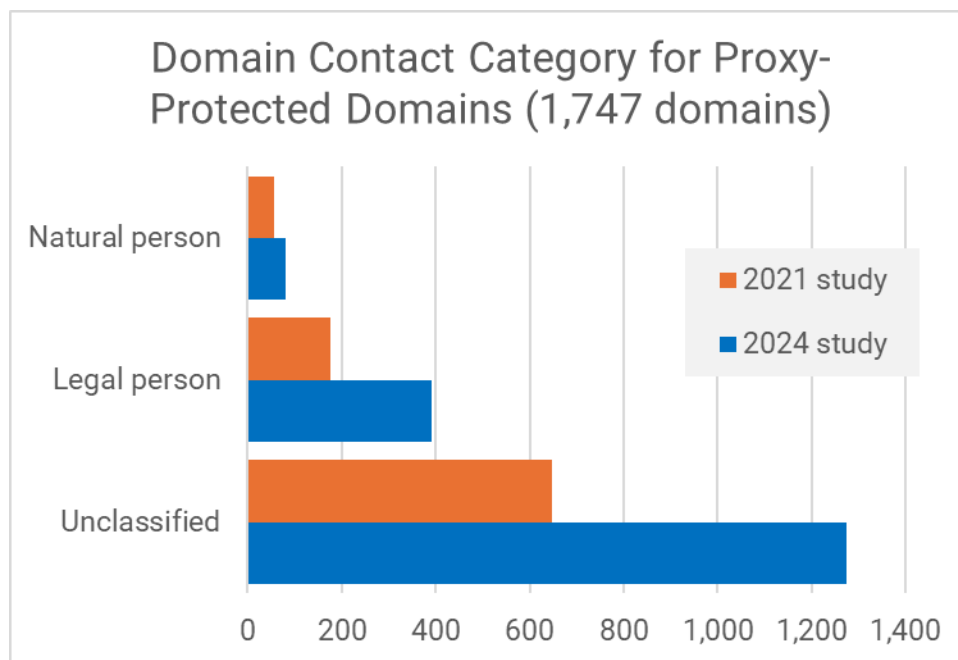
overwritten with proxy protection as registrars have applied blanket proxy protection to their domain portfolios.

The proxy service used to protect any given domain in nearly all cases was owned by the associated registrar. For example, the proxy-protected domains in GoDaddy's portfolio are under Domains By Proxy, LLC, which is owned by GoDaddy. The use of non-associated proxy services appears to be rare – we found only five domains where the proxy service used might not be owned by the domain's sponsoring registrar.

Proxy-Protected Registrants

The 2024 study set contained 1,747 proxy-protected domains, compared to 877 in the 2021 set. Of the 1,747 proxy-protected domains:

- 472 of the domains (27.0%) had users who identified themselves on their web sites. Of those:
 - 391 were legal persons, as confirmed by their web sites.
 - 81 were natural persons, as confirmed by their web sites.



In most cases the legal persons identified themselves on their web sites with specific contact data such as street address and phone number. Many gave the names of company personnel. Many included links to their social media accounts, especially at LinkedIn, Facebook, Instagram, and X.

We were unable to classify the registrant type for the remaining 1,275 proxy-protected domains. Of those, 166 proxy-protected domains resolved to user-created content, often of a commercial nature, but we could not determine whether the site user was a natural or legal person. For example, some were Etsy and Shopify stores, and we could not tell if the registrant was incorporated or not. Some did not offer any identifying information.

The other 1,109 did not offer content that could be used to identify a registrant type, including:

Type of non-identifying site	Number	% (of 3,000)
Parking pages	486	16.2%
Did not resolve (NXDOMAIN)	226	7.5%
Web site unreachable due to error (HTML error codes 4xx, certificate errors, etc.)	152	5.1%
“Under construction” pages	104	3.5%
“Domain for sale” pages	87	2.9%
Had malware or phishing; some were flagged with interstitial warning pages	24	0.8%
Access blocked due to Chinese national law	14	0.5%
Blank pages	14	0.5%
“WHOIS verification pending” pages placed by registrars	2	0.1%

Reach of GDPR Based on Jurisdiction

In the study set, there were 6 domains in the set of 3,000 where we could not discern the country of the domain’s registrant or user. **We determined that at least 23.3% of the domains (699 out of 2,994) were subject to GDPR based on the jurisdictions of the parties involved.** This is consistent with our 2021 study, which found that 23.1% of domains were subject to GDPR.

- 377 domains (12.5% of all domains) had a registrant in the EEA.⁴⁵ This number is an under-count, because 57% of domains are under proxy protection and the registrants’ true countries are obscured.
- 378 domains (12.6% of all domains) had their registrar in the EEA.
- 81 domains (3.0% of all domains) had their registry operator in the EEA. Of the TLDs in our set, four registry operators are legally domiciled in the EEA.
- 172 domains (5.7% of all domains) had their back-end provider in the EEA.⁴⁶

The following chart illustrates the subsets and overlaps. The first row indicates that there were 2,301 domains that were completely outside the GDPR’s jurisdictional reach – the same as in our 2021 study.

⁴⁵ The last data set that ICANN published, in 2017, showed that 14.3% of registrants resided in the EEA countries. See <https://www.icann.org/en/system/files/files/cct-metric-2-11-01nov17-en.xlsx>

⁴⁶ For a list of registries and back-end providers in the EU/EEA, see *Appendix A: TLD Representation in Sample Set*.

The second row indicates there were 106 domains where *only* the registrant was in the EEA (and the registrar, registry, and back-end provider were *outside* the EEA). The last row indicates that only two domains had *all four* parties in the EEA.

Domain's Registrant in EEA	Domain's Registrar in EEA	Domain's Registry Operator in EEA	Domain's Registry Back-end in EEA	TOTAL Domains (out of 2,994)	% of GDPR-covered domains (699)	% of all domains
				2,301		76.9%
✓				106	15.2%	3.5%
	✓			104	14.9%	3.5%
		✓		22	3.1%	0.7%
			✓	137	19.6%	4.6%
✓	✓			236	33.8%	7.5%
✓		✓		10	1.4%	0.3%
✓			✓	10	1.4%	0.3%
	✓	✓		4	0.6%	0.0%
	✓		✓	18	2.6%	0.6%
		✓	✓	36	5.1%	1.2%
✓	✓	✓		4	0.6%	0.0%
	✓	✓	✓	1	0.1%	0.0%
✓		✓	✓	2	0.1%	0.0%
✓	✓		✓	19	2.6%	0.6%
✓	✓	✓	✓	2	0.1%	0.0%

While 23.3% of the domains (699 out of 2,994) were subject to GDPR, only 12.5% of all domains (373 domains out of 2,994) had a registrant that resided in the EEA. This illustrates that the GDPR's jurisdictional reach extends far beyond EEA residents. By protecting personal data processed within the EEA, the GDPR extends protection to almost twice as many domains as have registrants who live in the EEA.⁴⁷

Also of note:

- 134 domains (4.5% of all 3,000 domains) had the registrant in the EEA, but the registrar, registry operator, and back-end were outside the EEA.

⁴⁷ Some registrants register more than one domain name, so there is not a one-to-one ratio between registrants (data subjects) and domains. Because so little contact data is now available via RDDS, is not possible to establish what the ratio may be.

- 261 domains (8.7% of all domains) had both the registrant and the registrar in the EEA. This was more than a third (37.4%) of the GDPR-covered domains.
- There were 126 domains (4.2%) where the registrant was in the EEA but used a registrar outside the EU. Registrants in the EEA used registrars in the EEA 66% of the time.
- 127 domains (4.2% of all domains) had the registrar in the EEA, but the registrant outside the EEA. This demonstrates that registrars in the EEA did not have many registrants outside the EEA.
- 137 domains (4.5% of all domains) identified only the back-end provider in the EEA, while the registrant, registrar, and registry operator were outside the EU. This is because Team Internet acts as the back-end provider for several gTLDs, and the registrants in those TLDs are mostly outside the EEA.
- Of the 699 domains subject to GDPR, 153 had some identifiable (non-proxy) contact data present in RDDS – at least the Registrant Organization.

Of the 377 domains with registrants in the EEA, 13 had an identified (non-proxy) registrant contact in RDDS. Of the 13, 12 were legal persons. The 13 registrants might be ones who opted into RDDS publication – an option required by ICANN policy.⁴⁸ If so, the opt-in to publication rate was only 3.4%.

GDPR Jurisdiction of Redacted Domains

29.9% of the domains in the study set had redacted contact data (894 of 2,994). Of the 894 redacted domains:

- 43.5% (389 of 894) were subject to GDPR, and 56.5% (505 of 894) were not subject to GDPR.
- 24.7% (221 of 894) were redacted but the Registrant Organization was returned in RDDS output.

The RDDS records for redacted domains are supposed to reveal the Registrant Country, per ICANN policy. Most do, but some were redacted or blank, in violation of ICANN contract. Germany, Great Britain, the Netherlands, China, Denmark, and the U.S. were the most common countries present in domain registration data.

Reach of GDPR Based on Jurisdiction *and* Legal Character

To be covered by the GDPR, data must fall within the GDPR’s jurisdictional scope, *and* the data subject must be a natural person – the data of legal persons is not protected.⁴⁹ How many domains qualify for GDPR protection under these criteria?

⁴⁸ See paragraph 7.2.1, at <https://www.icann.org/resources/pages/gtld-registration-data-specs-en>

⁴⁹ GDPR Recital 14: “The GDPR “does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.”

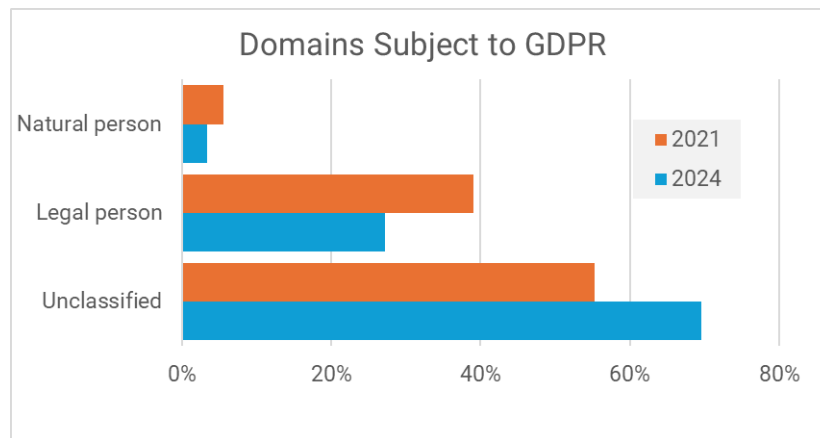
We determined that 699 domains in our study set of 3,000 (23.3%) were subject to GDPR based on jurisdictional scope, *i.e.*, on the confirmed location of the registrant, registrar, registry operator, or the back-end provider. That is the same proportion as we found in our 2021 study (23.1%, or 693 domains).

Of those 699 domains, 190 (27.2%) were with legal persons, 23 (3.3%) were with natural persons, and the other 486 (69.6%) were unclassifiable.

Fewer domain registrants were classifiable than in 2021. We attribute this to the extensive addition of proxy protection in recent years. Of the domains subject to GDPR, 63.4% (443 of 699) were under privacy/proxy protection. But in 2021, only 10.2% (74 of 699) were under privacy/proxy protection.

	2021	2024
Subject to GDPR	23.1%	23.3%
Natural person	5.6%	3.3%
Legal person	39.1%	27.2%
Unclassified	55.3%	69.6%

Fewer domains were redacted in 2024 data than in our 2021 study. For redacted domains, registrars are required to publish data in the Registrant Country field, making it possible for us to establish which of those registrants are in the EEA. Today, the prevalence of proxy protection obscures registrants' country of residence. Still, it is notable that in both 2021 and 2024, the percentage of domains subject to GDPR was similar, about 23%.



Some of the unclassifiable domains were registered by legal persons. How many is unknown, and the only way to determine how many is to obtain the proxy-protected and redacted contact data from the registrars. That is beyond the scope of this study.

The data shows that 89.2% of domains now have proxy-protected or redacted contact data. This is much larger than the 23.3% of domain names that fall under the jurisdiction of GDPR. While some

of this difference may be due to names which fall under other countries' similar privacy laws or trends in registrant demand for proxy services, registrars' increasing inclusion of proxy privacy as a standard feature is undoubtedly the most significant cause.

Let us make the conservative assumption that 50% of domains are registered by legal persons. As described above, at least 23.3% of gTLD domains are subject to GDPR based on jurisdictional scope. If half of those domains are registered by legal persons, then **the percentage of gTLD domains eligible for GDPR protection is around 11.6%**. That set consists of the natural person registrants located within the EEA, and natural person registrants who have their domain's registrar, registry, and/or registry back-end provider within the EEA. This is the percentage of domains that is necessary to protect under GDPR.

As noted above, the GDPR's reach extends far beyond EEA residents. By protecting personal data processed within the EEA, the GDPR extends protection to almost twice as many domains as have registrants who live in the EEA.⁵⁰ Extrapolated across the gTLD space, the GDPR's jurisdictional reach protects an estimated 23.2 million domains where the registrant does not live in the EEA.⁵¹

⁵⁰ Some registrants register more than one domain name, so there is not a one-to-one ratio between registrants (data subjects) and domains. Because so little contact data is now available in WHOIS, is not possible to establish what the domains-to-registrant ratio may be.

⁵¹ If 23.3% of domains are protected by GDPR, and 11.5% have a registrant in the EEA, then 11.8% of the protected domains are outside the EEA. The gTLD space consists of 221.5 million domains, and 221.5 million domains x 10.6% = 26.1 million.

NIS 2: Implications for Contact Data Availability

The NIS 2 directive will require that more identifiable contact data be available via RDDS, specifically that of legal persons. We estimate that in 2025, dependent on how the directive is transposed into Member State laws, perhaps 22.5% of domains *could* have actual, identifiable contact data available in RDDS, up from 10.8% currently.

The NIS 2 Directive⁵² is the new EU-wide⁵³ directive designed to promote a high common level of cybersecurity across the EU. NIS 2 entered into force on 16 January 2023, and each of the 27 EU Member States have until 17 October 2024 to transpose its measures into their national laws. The Member States may implement NIS 2 differently as long as their individual laws meet NIS 2's requirements. Individual Member States may also exceed NIS 2's requirements.

NIS 2 has specific requirements about domain registration services.

First, **NIS 2 specifies that registrars and registry operators *should publish* contact data in RDDS about legal persons, which is not considered “personal data” (and therefore, is not private) under GDPR⁵⁴:**

TLD name registries and entities providing domain name registration services should be required to make publicly available domain name registration data that fall outside the scope of Union data protection law, such as data that concern legal persons, in line with the preamble of Regulation (EU) 2016/679. For legal persons, the TLD name registries and the entities providing domain name registration services should make publicly available at least the name of the registrant and the contact telephone number. The contact email address should also be published, provided that it does not contain any personal data, such as in the case of email aliases or functional accounts. TLD name registries and entities providing domain name registration services 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.⁵⁵

⁵² NIS 2 full text: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555&qid=1709146869690#d1e3770-80-1>

⁵³ Note that while the GDPR applies to the entire European Economic Area (EEA) – including non-EU countries Norway, Iceland, and Liechtenstein – NIS 2 applies only to the EU's 27 Member States.

⁵⁴ See GDPR Recital 14, which states that GDPR “does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.”

⁵⁵ Preamble paragraph 112, Article 28 paragraph 4.

In addition:

- NIS 2 applies to any entity “which provide their services or carry out their activities within the Union”⁵⁶. This includes companies in the EU, and companies that offer registration services “to persons in one or more Member States”.⁵⁷ This is similar to GDPR.
- NIS 2 applies to domain name registries and registrars, “regardless of their size.”^{58, 59}
- NIS 2 applies to proxy and privacy providers. An “entity providing domain name registration services” means a registrar or an agent acting on behalf of registrars, such as a privacy or proxy registration service provider or reseller.”⁶⁰
- NIS 2 makes certain contact data fields mandatory to collect and to display in RDDS output. “Member States shall require the database of domain name registration data to contain the necessary information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs. Such information shall include:
 - (a) the domain name;
 - (b) the date of registration;
 - (c) the registrant’s name, contact email address and telephone number; and
 - (d) the contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant.”⁶¹

What are the practical implications? **More identifiable contact data should be published in the future** when the Member State laws become effective. Specifically, three sets of domains should go from proxy-protected or redacted to revealed in RDDS:

1. The contact data of any legal person in the EU should be published in RDDS, per the above requirements. This includes registrations made at any registrar outside the EU.
2. The contact data of any legal person that uses an EU-based registry, registrar, or reseller should be published in RDDS, per the above requirements.
3. NIS 2 applies to proxy and privacy providers. There are many domains under proxy protection that have no classifiable web site content. As a result, we cannot tell the registrants’ true country of residence. Some of these domains may be registered by legal persons in the EU and should have their contact data revealed.

How many domains in our 2024 study set are in cases 1 and 2 above?

⁵⁶ Article 2, paragraph 1.

⁵⁷ Preamble paragraph 116.

⁵⁸ Article 2 paragraphs 2(a)(iii) and 4).

⁵⁹ See also ICANN Organization’s comments on the pending NIS 2 legislation:

<https://www.icann.org/en/system/files/files/icann-org-comments-proposed-nis2-directive-19mar21-en.pdf>

⁶⁰ Article 6 paragraph 19.

⁶¹ Article 28 paragraph 2.

Case 1	Legal person registrant in EU; just Registrar in EU	90
Case 1	Legal person registrant in EU; with just Registry Operator and/or back-end in EU	7
Case 1	Legal person registrant in EU; registrar, registry, and back-end outside EU	45
Case 2	Legal person registrant outside of EU; just registrar in EU	30
Case 2	Legal person registrant outside of EU; just registry and/or back-end in EU	3
TOTAL		175

For case 3, we saw 1,067 domains that were unclassified, not under a provider in the EEA, and were under proxy protection. If we estimate that registrars outside the EEA have about 5% of their registrants in the EEA (5% of 1,067), then:

Case 3	Domains owned by Legal Persons in EEA, have proxy protection; registrar, registry Operator, and back-end are outside EEA	53
--------	--	----

Based on cases 1-3, at least an additional 7.6% of all gTLD domains should have contact data revealed in RDDS after NIS 2 goes into effect.

In the section “Reach of GDPR Based on Jurisdiction” above, we determined that at least 23.3% of gTLD domains are subject to GDPR based on the jurisdictions of the parties involved. If we estimate conservatively that half of domains are owned by legal persons, **then an additional 11.7% of gTLD domains (½ of 23.3%) should have contact data revealed in RDDS after NIS 2 goes into effect. Adding that to the 10.8% of domains that currently have contacts revealed, perhaps 22.5% of domains should have actual, identifiable contact data available in RDDS in 2025.**

This is an estimate based on incomplete data, especially because so many domains are owned by unidentifiable registrants, and because the effect of NIS 2 will also depend on registrar compliance with the law.

Appendix A: TLD Representation in Sample Set

Registry operators or back-end providers located in the EU/EEA are noted below.

The Domains in Registry data were obtained on 8 January 2024.

TLD	TLD Type	Domains in Registry	Market Share, of all gTLDs	Domains in Study Set	% of Sample Set	Registry Operator	Back-end Registry Provider
.com	legacy	157,804,215	72.0%	2,000	66.7%	Verisign	Verisign
.net	legacy	12,918,021	5.9%	219	7.3%	Verisign	Verisign
.org	legacy	10,776,135	4.9%	146	4.9%	PIR	Identity Digital
.info	legacy	3,641,507	1.7%	62	2.1%	Identity Digital	Identity Digital
.xyz	nTLD	3,283,935	1.5%	56	1.9%	XYX.COM LLC	Team Internet (CentralNIC)
.online	nTLD	2,857,201	1.3%	48	1.6%	Radix	Team Internet (CentralNIC)
.top	nTLD	2,663,430	1.2%	45	1.5%	Jiangsu Bangning	ZDNS
.shop	nTLD	2,183,561	1.0%	37	1.2%	GMO Registry	GMO Registry
.site	nTLD	2,008,616	0.9%	27	0.9%	Radix	Team Internet (CentralNIC)
.store	nTLD	1,357,081	0.6%	23	0.8%	Radix	Team Internet (CentralNIC)
.biz	legacy	1,257,246	0.6%	21	0.7%	Registry Services, LLC (GoDaddy)	GoDaddy
.cf	nTLD	1,019,406	0.5%	21	0.7%	DotCFD Registry/Boston Ivy	Team Internet (CentralNIC)
.vip	nTLD	844,943	0.4%	20	0.7%	Registry Services, LLC (GoDaddy)	GoDaddy
.app	nTLD	668,382	0.3%	20	0.7%	Charleston Road (Google)	Charleston Road (Google)
.club	nTLD	583,818	0.3%	20	0.7%	Registry Services, LLC (GoDaddy)	GoDaddy
.live	nTLD	584,738	0.3%	20	0.7%	Identity Digital	Identity Digital
.click	nTLD	561,099	0.3%	20	0.7%	Internet Naming Co.	Tucows
.tech	nTLD	462,599	0.2%	20	0.7%	Radix	Team Internet (CentralNIC)
.pro	Legacy	485,299	0.2%	20	0.7%	Identity Digital	Identity Digital

TLD	TLD Type	Domains in Registry	Market Share, of all gTLDs	Domains in Study Set	% of Sample Set	Registry Operator	Back-end Registry Provider
.dev	nTLD	403,969	0.2%	20	0.7%	Charleston Road (Google)	Charleston Road (Google)
.icu	nTLD	385,425	0.2%	20	0.7%	Shortdot SA	Team Internet (CentralNIC)
.cloud	nTLD	335,360	0.2%	20	0.7%	Aruba S.p.A.	Tucows
.asia	nTLD	305,773	0.1%	20	0.7%	DotAsia Organisation	Identity Digital
.link	nTLD	226,204	0.1%	20	0.7%	Nova Registry	Tucows
.tokyo	nTLD	109,837	0.1%	20	0.7%	GMO Registry	GMO Registry
Total		207,199,116	95%	3,000			

The registry operators and back-end providers legally established in the EEA are in **boldface**, below:

- .CFD (registry operator **DotCFD Registry in U.K.**, back-end **Team Internet in U.K.**)
- .CLOUD (registry operator **Aruba PEC S.p.A. in Italy**, back-end Tucows in Canada)
- .ICU (registry operator **ShortDot in Luxembourg**, back-end **Team Internet in U.K.**)
- .LINK (registry operator **Nova Registry in Malta**, back-end Tucows in Canada)
- .ONLINE (registry operator DotOnline Inc. in the United Arab Emirates, back-end **Team Internet in U.K.**)
- .SITE (registry operator DotSite Inc. in the United Arab Emirates, back-end **Team Internet in U.K.**)
- .STORE and .TECH (registry operator Radix in the Cayman Islands, back-end **Team Internet in U.K.**)
- .XYZ (registry operator XYZ.COM LLC in U.S., back-end **Team Internet in U.K.**)

The European Economic Area (EEA) consists of the Member States of the European Union (EU), plus three countries of the European Free Trade Association (EFTA): Iceland, Liechtenstein, and Norway. Although the United Kingdom has “Brexit” the European Union, we counted the U.K. as being under GDPR because the U.K. followed GDPR in 2020, and the U.K. also has its own parallel data protection act that is modelled directly on the GDPR.

Appendix B: Registrar Representation in Sample Set

Below is data for the twenty largest registrars.

The Registrar Domains Under Management (DUM) was obtained from ICANN Monthly Registry Reports⁶² for October 2023.

Registrar IANA ID	Registrar	Registrar DUM	Domains in Study Set	% of Study Set	% of Market
146	GoDaddy.com	66,048,308	844	28.1%	28.7%
1068	Namecheap	16,138,187	229	7.6%	7.0%
69	Tucows Domains	9,922,847	147	4.9%	4.3%
895	Squarespace Domains II LLC	9,460,029	114	3.8%	4.1%
49	GMO Internet Group d/b/a Onamae.com	5,001,879	87	2.9%	2.2%
2	Network Solutions	5,126,007	67	2.2%	2.2%
83	IONOS SE	4,734,076	64	2.1%	2.1%
1441	TurnCommerce DBA NameBright.com	4,888,575	63	2.1%	2.1%
1923	Gname.com	4,285,751	61	2.0%	1.9%
303	PDR d/b/a PublicDomainRegistry.com	4,431,131	58	1.9%	1.9%
1479	NameSilo	4,641,199	52	1.7%	2.0%
48	eNom	3,963,106	52	1.7%	1.7%
472	Dynadot	3,488,826	48	1.6%	1.5%
1599	Alibaba Cloud Computing d/b/a HiChina	3,219,314	44	1.5%	1.4%
1636	HOSTINGER operations	2,063,617	40	1.3%	0.9%
3817	Wix.com	2,768,148	40	1.3%	1.2%
420	Alibaba Cloud Computing (Beijing)	2,677,411	32	1.1%	1.2%
440	Wild West Domains	2,477,563	32	1.1%	1.1%
625	Name.com	2,221,010	31	1.0%	1.0%
299	CSC Corporate Domains	1,436,887	29	1.0%	0.6%

⁶² <https://www.icann.org/resources/pages/registry-reports>

About Interisle Consulting Group, LLC

Interisle's consultants are experienced practitioners with extensive track records in industry and academia and world-class expertise in business and technology strategy, Internet technologies and governance, financial industry applications, and software design. For more about Interisle, please visit: www.interisle.net

About the Authors

Greg Aaron is an internationally recognized authority on the use of domain names for cybercrime, and is an expert on DNS policy, investigations and due diligence, and related intellectual property issues. He works with industry, researchers, and law enforcement to investigate and mitigate cybercrime, and is also a licensed private detective. As a member of ICANN's Security and Stability Advisory Committee (SSAC), he advises the international community regarding the domain name and numbering system that makes the Internet function. Mr. Aaron is Senior Research Fellow for the Anti-Phishing Working Group, where he edits the APWG's quarterly metrics reports. He has managed multiple top-level domains around the world, including .INFO, .ME, and .IN. He was the senior industry expert on a team that evaluated the policy and technical qualifications of more than one thousand new TLD applications to ICANN in 2012-2013. He is President of Illumintel, Inc., a consulting company. Mr. Aaron is a *magna cum laude* graduate of the University of Pennsylvania.

Lyman Chapin has contributed to the development of technologies, standards, and policy for the Internet since 1977, and is widely recognized and respected as a leader in the networking industry and the Internet community. Mr. Chapin is a Life Fellow of the IEEE, and has chaired the Internet Architecture Board (IAB), the ACM Special Interest Group on Data Communication (SIGCOMM), and the ANSI and ISO standards groups responsible for Network and Transport layer standards. Mr. Chapin was a founding trustee of the Internet Society, and a Director of the Internet Corporation for Assigned Names and Numbers (ICANN). He currently chairs ICANN's Registry Services Technical Evaluation Panel (RSTEP), which is responsible for assessing the impact of new Domain Name System (DNS) registry services on the security and stability of the Internet, and the DNS Stability Panel, which evaluates proposals for new Internationalized Domain Names (IDNs) as country code top-level domains (ccTLDs). He is also a member of ICANN's Security and Stability Advisory Committee (SSAC). He has written many other papers and articles over the past 40 years, including the original specification of the Internet standards process operated by the IETF. Mr. Chapin holds a B.A. in Mathematics from Cornell University.

David Piscitello has been involved in Internet technology and security for more than 40 years. Until July 2018, Mr. Piscitello was Vice President for Security and ICT Coordination at ICANN, where he participated in global collaborative efforts by security, operations, and law enforcement communities to mitigate Domain Name System abuse. He also coordinated ICANN's security capacity-building programs, and was an invited participant in the Organisation for Economic Co-operation and Development (OECD) Security Expert Group. Dave is an Associate Fellow of the Geneva Centre for Security Policy. He served on the Boards of Directors at the Anti-Phishing Working Group (APWG) and Consumers Against Unsolicited

Commercial Email (CAUCE). He is the recipient of M3AAWG's 2019 Mary Litynski Award, which recognizes the lifetime achievements of individuals who have significantly contributed to making the Internet safer.

Dr. Colin Strutt has published and spoken extensively on networking technology, name collisions, enterprise management, eBusiness, and scenario planning, and has represented the interests of Digital Equipment, Compaq, and the Financial Services Technology Consortium in national and international industry standards bodies. He holds six patents on enterprise management technology and brings more than thirty five years of direct experience with information technology, as a developer, architect, and consultant, with recent work including design and operation of a regional public safety network, providing technical expertise relating to patents, and analysis of world-wide Internet use. Dr. Strutt holds a B.A. (with First Class Honours) and Ph.D. in Computer Science from Essex University (UK).