Council of European National Top-Level Domain Registries

Registration data accuracy in European national domain registries: existing practices and challenges

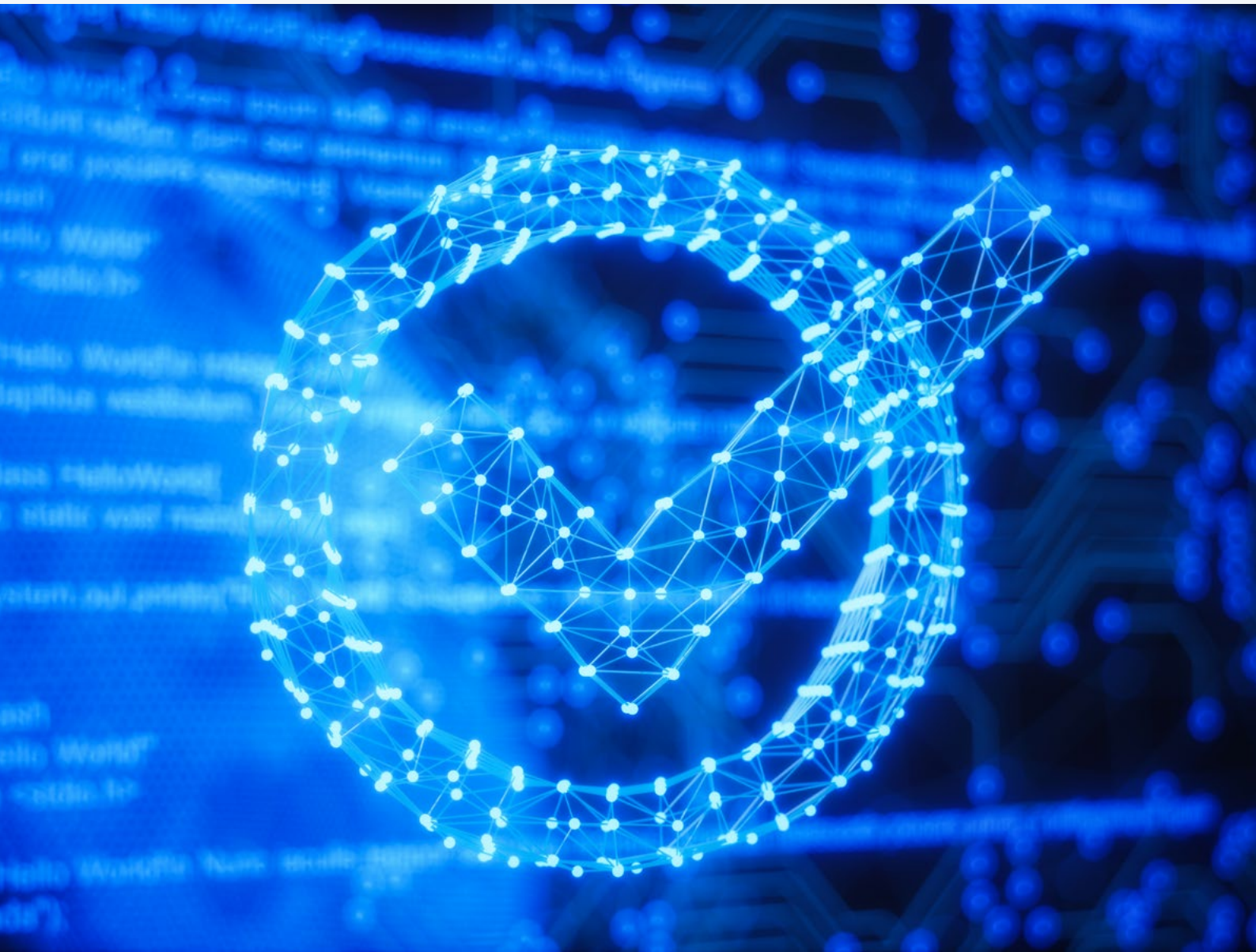


Table of contents

Key terms

The following key terms will be used for the sole purpose of improving the legibility of this paper and are defined as follows:

Data accuracy	the measure of the likelihood that information about a registrant is correct.
Data validation	data validation ensures that data complies with the expected format. It typically comprises syntax checks (i.e. postal code) or the formatting of email addresses.
Data verification	data verification evaluates whether data correctly reflects the attributes of the registrant (such as their identity or postal address). It aims to establish the accuracy of the claimed identity of the registrant.
Registrant identification data	datasets which consist of the personal data of registrants, such as their name, email address, postal address and phone number.
Reachability check	process which checks whether registrants can be reached via the provided email address and/or phone number (usually conducted via e-mail or SMS).
Syntax check	process which checks that the information provided is in the correct format (i.e. phone number with a valid country-code and within the character limits).

Executive summary

This White Paper addresses the topic of maintaining registration data accuracy in European national top-level domain registries (ccTLDs). Registration data accuracy has become a regulatory topic at national and European levels, as evident from the recent finalisation of the NIS 2 Directive negotiations that introduce data accuracy obligations on domain name registries and entities providing domain name registration services in the EU. The aim of this White Paper is to shed light on existing practices of maintaining domain name registration databases accurate and up to date across European ccTLDs. These existing practices may serve as guidance for the domain name industry, policymakers, law enforcement authorities and CSIRTs when addressing the implementation of the NIS 2 Directive.

Key findings

- To perform their essential function within the Domain Name System (DNS), registries need to maintain a list of the domain names in their zone (such as .eu). Those domain names are mapped against a list of IP addresses. Data protection principles, such as data minimisation, have guaranteed that only data that is essential for the performance of this service is collected and processed.
- Registries collect registrant identification data (such as the registrant's name, email address, postal address and phone number) to ensure accurate administrative information on the domain name holder and the various contacts associated with it, to announce changes to technical and legal terms, to notify registrants about important domain life cycle events (such as renewal), or about security incidents involving their domain name. Typically registrant data is collected by registrars (or resellers) who provide this data to the registry under the terms set forth in the registry-registrar contract.
- Data accuracy within the domain name space refers to a set of various technical, contractual and regulatory obligations. Registrant identification data verification is only a subset of the overall accuracy discussion when it comes to the DNS. Despite increased regulatory attention towards registrant identification data verification, accuracy discussions within the domain name space require a careful equilibrium between all compliance areas applicable to domain name registries.
- Registrant identification data collection, validation and verification practices differ across European ccTLDs, depending on local requirements and restrictions or the relevance (e.g. language) or availability (e.g. eID) of specific data sets. Due to these local particularities, there is no guarantee that simply adopting one policy or method from a country will lead to the same results in another country.
- European ccTLDs have consistently been referred to as providing the 'best practices' on tackling a variety of societal concerns, such as wider cybersecurity and promoting trust online, despite the absence of uniform practices for addressing registration data accuracy.
- The diversity in process and policies related to registration data accuracy provides structural strength to the European DNS space as it avoids single points of failure and creates a marketplace of ideas that encourages innovation.

- A range of solutions exist in the CENTR community to ensure the validation and verification of registration data, that in particular depend on the digital maturity of national eID infrastructures, as well as local payment services and market conditions.
- Based on the results of a survey run by CENTR in 2022, around 50% of the 33 respondents perform data validation through syntax checks on the received registration data. Only a handful of registries verify data proactively.
- The majority of European ccTLDs perform registrant identification data verification checks on an ad hoc basis. The reasons why systematic proactive identification data verification is not common among registries may be explained by the fact that it requires significant human resources, as automatic checks for identity are unavailable and often unreliable. Technical syntax checks on the other hand are generally automated and easy to implement.
- According to the CENTR survey, only 5 registries out of the 33 respondents currently have relevant eID methods in place for verifying registrants. The availability of national eID solutions is limited and not available for cross-border use, making it challenging to use within the European domain space.
- The majority of European ccTLDs do not limit their registration eligibility criteria to residents of their country, meaning that domain names within their ccTLD are also available for registration across the EEA and outside the EU. The automated and reliable verification of foreign registrants remains a challenge.
- The verification of contact details, such as email addresses, postal addresses and phone numbers is challenging. If in some cases an accurate and most up-to-date postal address could be verified by requiring the submission of utility bills or sending registered letters to an indicated postal address, it is virtually impossible to verify if email addresses and phone numbers belong to the person that claims to be the registrant.
- A risk-based approach towards registrant identification data verification is generally considered to be a more proportionate approach, rather than a blanket and general verification requirement targeted at all registrants.
- Registries generally consider it to be the registrar's responsibility to collect and share all necessary registration data with them, as well as to ensure the validation and verification of that data. The NIS 2 Directive aims to reduce the duplication of data accuracy efforts between registries and registrars. It might be worth clarifying at national level within the implementation phase that this NIS 2 requirement should only concern the verification obligation to alleviate the burden on domain holders to provide additional identification information to multiple entities.
- Considering national specificities, it would be desirable to allow flexibility for registries and registrars in choosing their verification methods, as technological solutions are changing quickly. For these reasons, the implementation of the NIS 2 Directive and any revision of national rules should stay technologically neutral and not prescribe any methods on how to comply with accuracy-related provisions, in the interest of future-proof policymaking.

Introduction

What is domain name registration data?

Domain names provide a human-readable interface for navigating the internet, whereas computers and other digital devices require internet protocol (IP) addresses to be able to interact with each other.

The mapping between registered human-readable domain names and IP addresses is supported by domain name registries, such as ccTLDs. To perform their essential function, registries do not need to retain a lot of data. They need to have a list of domain names and for each domain name a list of nameservers, which, in turn will map the "delegated" domain name space to IP addresses that helps individuals and businesses find the right resources.

Additional technical data may be retained by registries to enable certain security features such as DNS Security Extensions (DNSSEC) or registry lock. DNSSEC data is a cryptographic scheme that enables the validation of the authenticity of DNS data. Registry lock is a flag that can be set to let the registry know that it should not allow changes to the domain name data without secondary checks. Those checks often involve additional contacts for the domain name beyond the registrant.

However, for the administrative processing of the contractual relationship between the holder of the domain name (*the registrant*) and the domain name registry, additional information is collected and processed. Which data is required to be collected differs between the registries, according to their respective terms of service. Often this data is collected by a *registrar*, who acts as a sales channel for the registry. In this White Paper we will refer to this set of data as '*registrant identification data*'. This data typically consists of the personal data of registrants, such as their name, email address, postal address and phone number.

What is registration data accuracy?

Registration data accuracy generally refers to several technical requirements and legal obligations, as enshrined in national and EU law, relevant for the domain name space.

It may describe the data accuracy mandated by European data protection law in relation to the protection of private persons and their right to request the rectification of incorrect personal information.[1] It may also describe data accuracy foreseen in the DNS space that relates to the accuracy of data kept in databases according to technical requirements.[2]

1 Article 5(1)(d) of the General Data Protection Regulation of the European Union (GDPR) and associated national implementations.

2 RFC 1591: "The designated manager must do a satisfactory job of operating the DNS service for the domain. That is, the actual management of the assigning of domain names, delegating subdomains and operating nameservers must be done with technical competence. This includes[...] operating the database with *accuracy*, robustness, and resilience"[emphasis added].

Finally, it may describe data collection resulting from regulatory requirements such as the verification of the identification data of individuals and legal entities registering domain names, as envisaged in the upcoming EU NIS 2 Directive.[3]

When policy discussions refer to registration data accuracy, it is the verification of registrant *identification* data that is usually being referred to. Here it is noteworthy that after increased regulatory attention towards registrant identification data verification, accuracy discussions within the domain name space require a careful equilibrium between all three areas mentioned above of obligations applicable to domain name registries. Accuracy in the context of domain name registration data is not a binary issue but rather a measure of the likelihood that the registrant provided sufficiently accurate information.

Registrant identification data collection, validation and verification practices differ across European ccTLDs, depending on local requirements and restrictions or the relevance (e.g. language) or availability (e.g. electronic identification or eID) of specific data sets.

While the NIS 2 Directive data accuracy obligations aim to harmonise the minimum dataset of registrant identification data that needs to be maintained accurate, complete and up to date, including by verification, the importance of maintaining the variety of different data accuracy practices across European ccTLDs cannot be underestimated.

In Europe, ccTLD operators vary considerably in business model, ownership, size and relations with their governments. Most ccTLDs are not-for-profit: foundations, cooperatives, universities, research institutes and public institutions. By nature, ccTLDs have strong links with their local internet communities, including the government. ccTLDs are mainly governed by national and regional (e.g. EU) law.

ccTLDs set their own terms and conditions (T&C). These policies concern the duration of the registration period, the prices, terms of use, prohibited names, and in some cases local presence requirements.

Some ccTLDs have restrictions on their customer base. There are cases where only residents of a particular country can register domains with the national ccTLD registry[4], or there are limits on the number of domains registered per one registrant within that national ccTLD.[5] In the EU, access to TLDs needs to be granted for all potential EU-based domain name holders.

Several registries have national legal and/or administrative requirements regarding the accuracy of domain name registrant data. Notable examples are Denmark[6], Sweden[7], Spain[8] that include domain name specific national legislation that includes accuracy-related provisions applicable to the respective ccTLD.

---

3 Article 23 of the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 ('NIS 2 Directive'), COM/2020/823 final, December 2020.

4 AuDA Domain Name Eligibility and Allocation Policy Rules for the Open 2LDs, Schedule A, §2; Norid Domain name policy, §5.3.

5 Norid Domain name policy, §5.4.

6 Domain Name Act, LOV nr 164 af on 26 February 2014.

7 The Swedish Top-level Domains Act (2006:24).

8 The Domain Names National Plan under the country code for Spain (".es").

CENTR members all have unique ways of addressing their roles in the technical ecosystem and local regulatory conditions. It is important to note that no uniform practice for addressing registration data accuracy exists. Due to the local particularities, there is no guarantee that simply adopting one policy or a method from one country will lead to the same results in another. Notwithstanding European ccTLDs have consistently been referred to as providing 'best practices' on tackling a variety of societal concerns beyond their essential function to maintain a robust and stable internet infrastructure service.[9]

It should be noted that this diversity in process and policies provides a structural strength to the European DNS space. Not only does diversity avoid single points of failure, but most importantly, it creates a marketplace of ideas that encourages innovation.

9 Europol, "Spear Phishing, A Law Enforcement and Cross-Industry Perspective", 2019; European Commission, "Study on Domain Name System (DNS) Abuse", 2022.

The collection and verification of registrant identification data

Under European data protection law, data accuracy is verified by the data subject, whose right it is to bring to the attention of a data controller that data needs to be rectified.[10] Data accuracy discussions within the domain name space, however, concern the obligation on registries, registrars and other parties to ensure that potential data subjects *provide* correct data.

In data accuracy regulatory discussions, such as the NIS 2 Directive, the burden of proof is therefore reversed as compared with data protection laws. The verification obligation that will be applicable to registries and registrars under the NIS 2 Directive will introduce additional validation requirements for domain name registrants, including in some cases by submitting more personally identifiable information than is currently needed to provide domain name services.

Collected registrant identification data is used to ensure accurate billing for registration and renewal fees, for announcing important changes in technical services or legal terms of service, as well as for notifications on the important events within a domain name life cycle (i.e. renewal) or about security incidents involving their domain name, and in some cases for countering abuse such as phishing, spam and other unlawful activities. Registries may require this data from registrars, who collect it to fulfill their terms and conditions with the registry.

The verification of the data can be done by ensuring accurate billing (i.e. that fees are paid when they are due), by verifying collected data by consulting relevant public databases, through manual follow-up with individual data subjects, automated syntax checks or by requiring the authentication of data entry with a national electronic identification (eID). A range of solutions exist in the CENTR community, that in particular depend on the digital maturity of national eID infrastructures, as well as local payment services and market conditions.

Concrete datasets

Registrant identification data is any data that allows the registry to identify and contact the registrant. The information collected will typically differ when the registrant is a legal entity compared to the situation when the registrant is a natural person. According to the upcoming NIS 2 Directive, ccTLDs and entities providing registration services, such as registrars, should collect and maintain accurate and complete domain name registration data in a dedicated database. It shall contain the registrant's full name, contact email address, contact telephone number, as well as the contact email and phone number of the point of the contact administering the domain name in case it is different from the registrant's.

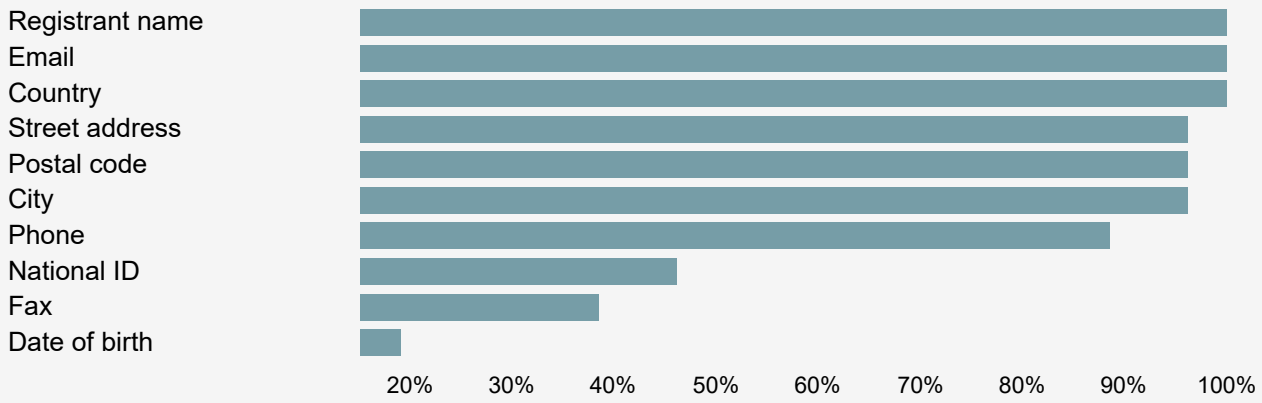
Based on a CENTR survey (2022), out of 33 respondents, 70% of European ccTLD registries make a distinction between domain name registrations made by legal entities and natural persons.

For natural persons registrants, 100% of the surveyed members collect the registrant full name and email address. Similarly for legal entities, 100% of surveyed members collect the organisation and/or company name and email address.

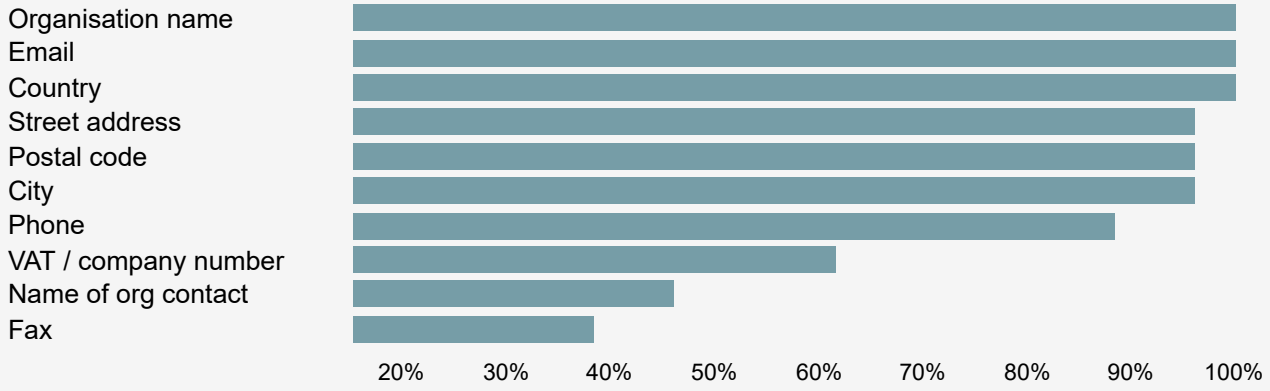
10 Article 5(1)(d) of EU GDPR.

DATA COLLECTED

For a natural person at the time of registration



For a legal entity at the time of registration



Note that the above fields may be collected by registries as mandatory or optional fields.
'National ID' may include other forms of personal identification. 'Postal details' include street address, city, country and postal code.
Sample: 26 CENTR member registries. Source: CENTR

Other common datasets include postal address and phone number.

Some European ccTLDs collect additional data such as language, IBAN, business category, VAT or enterprise number. What is collected depends on local legal requirements or restrictions.

The collection of this data is necessary for the performance of the contract to which the data subject is a party upon registering a domain name. The data is submitted by the registrant during the registration process via the registrar. It is in the interest of the registrant to provide accurate data in order to establish any legal rights related to the registration of the domain name.

The majority of respondents indicated that based on contractual provisions the registrar is responsible for the collection of the registration data and ensuring its accuracy. However, according to the survey respondents, these contractual provisions are seldom enforced. This might be due to the fact that it is generally considered to be the responsibility of a domain name holder to provide accurate identification data. 78% of the surveyed registries have requirements on their registrars to validate registrant details. Common terms used in registrar agreements require registrars “to make reasonable efforts” to ensure the accuracy of registration data collected from registrants.

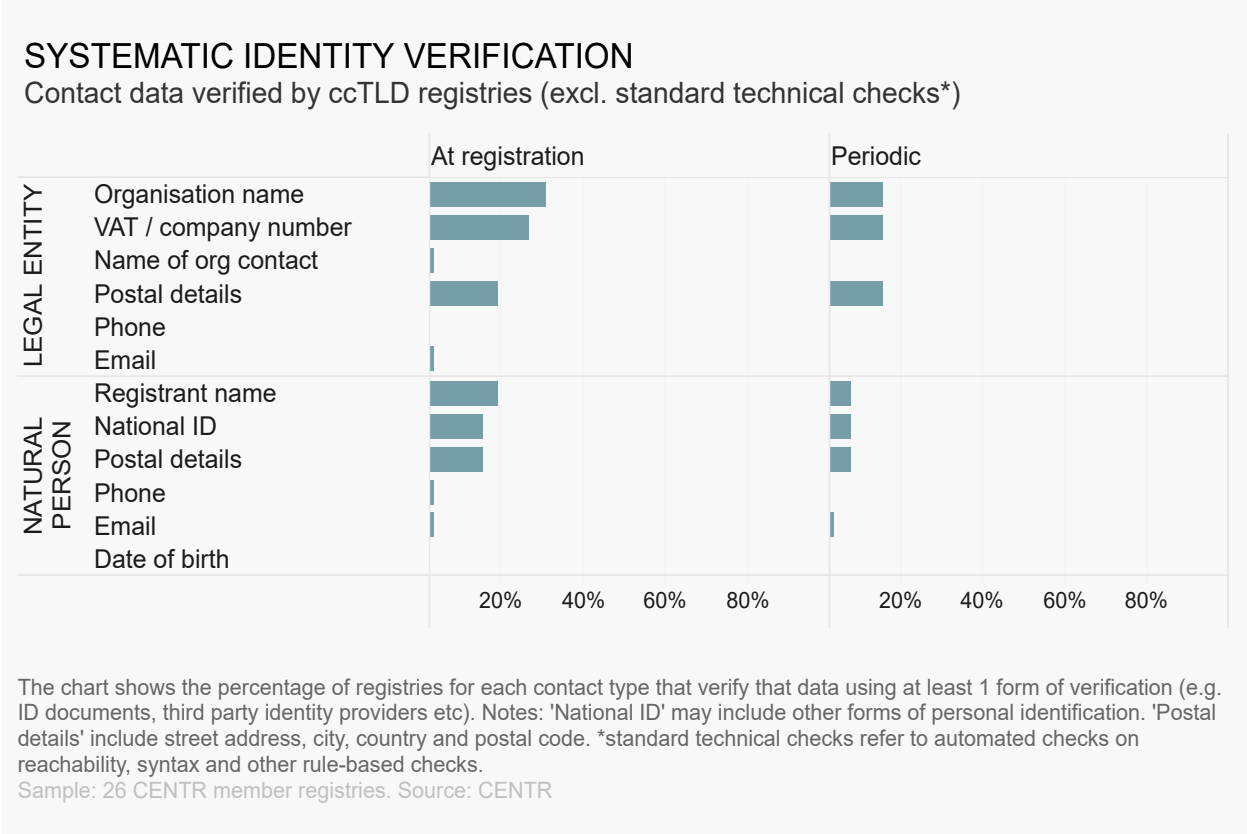
Validation vs verification

For the purpose of this White Paper we make a distinction between two levels of accuracy checks: data *validation* and data *verification*.

Data validation assures that the data complies with the expected format. Validation typically comprises syntax checks such as postal code checks or the formatting of email addresses.

Data verification evaluates if the data correctly reflects the attributes (such as identity or postal address) of the registrant. Data verification aims to establish the accuracy of the claimed identity of the registrant.

Around 50% of the respondents in the CENTR survey reported performing data validation through syntax checks on the received registration data. Only a handful of registries verify data proactively. Verification is typically done on an ad hoc basis.



The chart shows the percentage of registries for each contact type that verify that data using at least 1 form of verification (e.g. ID documents, third party identity providers etc). Notes: 'National ID' may include other forms of personal identification. 'Postal details' include street address, city, country and postal code. *standard technical checks refer to automated checks on reachability, syntax and other rule-based checks.
Sample: 26 CENTR member registries. Source: CENTR

Timing of verification

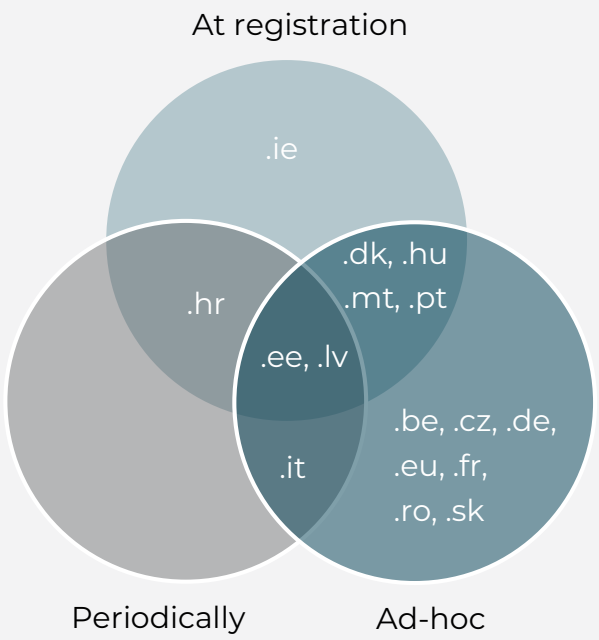
Data verification is an additional hurdle in the registration process. At a time when it takes minutes to create a profile on any social media platform, it is essential that domain name registration is as frictionless as possible. Data verification requires additional human resources, since automated processes are often absent: the effect of manual verification could result in delays of multiple days before the registrant can start using their domain name.

For those ccTLDs that do perform registrant identification data verification, it is done mostly on an ad hoc basis. This means that there are only a few registries for which data is being proactively verified.

There is no conclusive information on how often these ad hoc verifications occur as they are generally based on events such as a complaint or the failure of a technical check. The most common events which trigger an ad-hoc verification procedure are: third party complaints, change of registrar, failure of technical check and incomplete data.

Timing of data verification

Registry included if a minimum of one data field is verified



*Excludes all technical checks

Methods of verification

The most common means used in registrant data verification are lookups in external databases which may also be linked to third-party validation providers. For example, using the VAT Information Exchange System (VIES) could be considered both an external database lookup as well as a third party identity validation provider.

Overall, the most common methods of verification are:

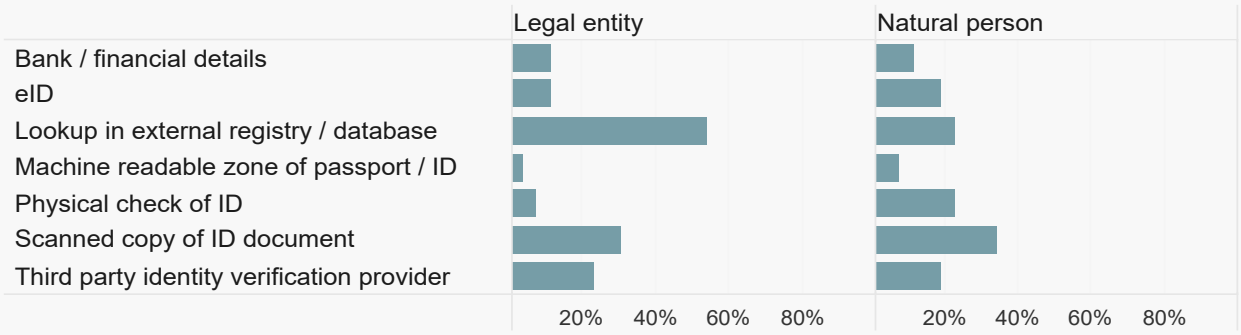
- Legal entities: lookup in an external database and/or third party validation provider
- Natural persons: scanned copy of an ID document

The least common verification tools across all registrant types are:

- Machine-readable zone (MRZ) of a passport or ID (used by 2 respondents)
- Bank details (used by 3 respondents)
- Electronic identification (eID) (used by 5 respondents)

VERIFICATION TOOLS USED

Methods used by ccTLD registries to verify contact data



The chart shows the percentage of registries using each method of contact data verification to verify some part of the contact's details (e.g. name, email etc). Chart excludes technical checks such as syntax, rule-based etc.
Sample: 26 CENTR member registries. Source: CENTR

Third-party identity providers are reported to be used by 6 (18%) registries. For both local and foreign identity verification, the most commonly referred service was VIES (VAT Information Exchange System).

Few registries offer a platform whereby registrants can verify their registration data.

53% of registries stated that their verification process has changed over the past few years. For most, there has been an increase in efforts to validate more data fields. 47% of registries are also either planning or have plans to change how data is verified in the future.

FUTURE PLANS

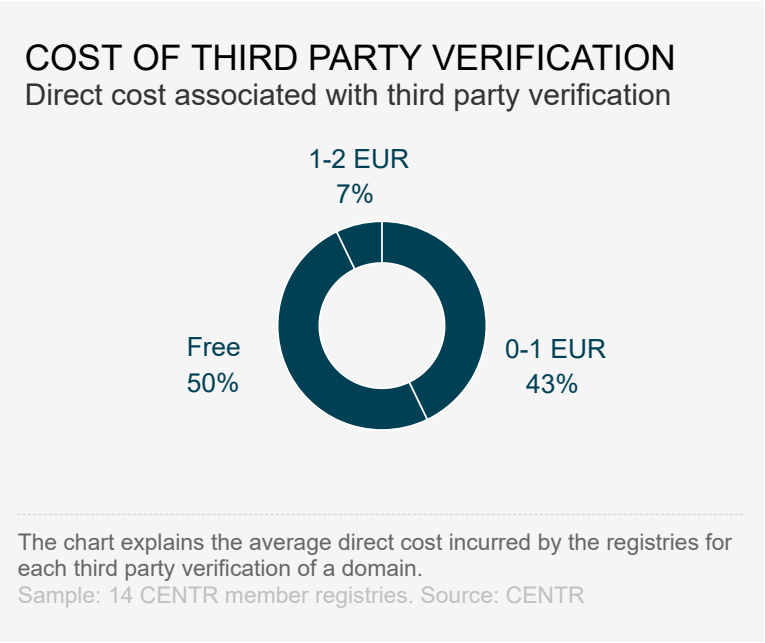
Registries' plans to change / expand how data is validated or verified

Planning	Possible	Not planning	Unsure
35%	23%	19%	23%

The chart explains future plans of registries regarding changing / expanding how data is validated or verified.
Sample: 26 CENTR member registries. Source: CENTR

The survey also asked the respondents to provide costs associated with using third party services[11] For only 42% of registries the cost is free. Note that this may be influenced by the fact that VIES is a free search service used by several registries. However, this only covers the verification of legal entities. Depending on how each Member State implements the NIS 2 Directive and due to the fact that there are no silver bullet solutions for verifying all required data fields under the upcoming NIS 2 Directive obligations, costs for data verification performed by registries will most likely increase.

11 Note that 19 responses were received to the question on third party costs. This figure conflicts with a previous question on how data is validated suggesting a potential error in the interpretation of the question on cost.



The chart explains the average direct cost incurred by the registries for each third party verification of a domain.
Sample: 14 CENTR member registries. Source: CENTR

Experiences from European ccTLDs

As evident from the empirical analysis above, the majority of European ccTLDs perform registrant identification data verification checks on an ad hoc basis. The reasons why systematic identity verification is not common among registries may be explained by the fact that it requires significant human resources, as automatic checks for identity are unavailable and often unreliable. Technical syntax checks on the other hand are generally automated and easy to implement.

European ccTLDs in general prefer to limit verification of identification data to cases which are flagged, either by internal tools and/or complaints. This allows them, as technical infrastructure operators, to achieve the necessary balance between ensuring their essential service for the benefit of society and contributing to the overall trust in their domain space.

DNS Belgium (.be) conducts registrant verification checks on newly-registered .be domain names that have been flagged suspicious through the use of a rule based system (if a new registration triggers a certain amount of hit points it is selected for registrant verification) and which are not delegated before the proof of identity of a registrant is received. Registrants can verify their identity automatically without DNS Belgium's staff interference via electronic identification methods available on DNS Belgium's website. However, the automatic use of electronic identification methods is not always feasible, and registrants can resort to an alternative verification method that requires manual verification performed by DNS Belgium's staff.

DK Hostmaster (.dk) requires registrants that are resident in Denmark to identify themselves using the Danish national eID – NemID - before the domain is delegated. DK

Hostmaster also cross-checks the registrant data of Danish residents with the national databases of the Civil Registration System (CPR) and Central Business Register (CVR).

SIDN (.nl) performs registrant verification checks on an ad hoc basis post-registration when there are reasons to suspect that a domain name is malicious. Once the suspicious registration is identified, the registrant is asked to provide proof of the registration data provided, such as a copy of ID for natural persons, or an extract from a business register for legal entities. If required proof is not provided within five days, the domain name is suspended.

Afnic (.fr) performs registrant checks on an ad hoc basis, requesting additional information from the registrant by e-mail. Natural persons are requested to provide a copy of an ID document and proof of postal address such as a utility bill. Legal entities are required to provide a certificate of incorporation in case of these ad hoc accuracy checks. The verification checks are entirely manual. The domain is blocked after seven days once the data accuracy verification process is triggered and deleted after 30 additional days if there is no response from the registrant. Starting from January 2023, Afnic will introduce a new verification procedure to block domain name registrations at the time of their creation, in case these do not comply with .fr eligibility criteria.

Internetstiftelsen (.se) contacts a registrant in the event of an alert or a suspicion that the registration data is false with a request to rectify the information. Failure to rectify this information will cause the domain name to be deactivated for a period of 60 days. During this period, the registrant will still be able to correct the flaw and re-enable the domain name. If this is not done, the domain name is deregistered. The registry allocates human resources to identify potentially inaccurate registration information within the .se zone.

Challenges with the general verification obligation

The use of electronic identification methods

Data accuracy obligations under the NIS 2 Directive allow some flexibility for registries to choose their method for verifying registrant identification data. According to the relevant explanatory provisions related to the data accuracy obligations in Article 23, registries and registrars should adopt and implement proportionate processes to verify registration data. These processes should reflect the current best practices used within the industry and, to the extent possible, the progress being made in the field of electronic identification (eID).[12]

According to the CENTR survey, only 5 registries out of the 33 respondents currently have relevant eID methods in place for verifying registrants.

Some of the obstacles in using eID for verifying registrant identification data that have been observed across the CENTR membership, include:

1. **Non-availability of public eID schemes that can be relied upon in verification checks.** Despite the EU eIDAS Regulation being in place since 2014, only 18 EU Member States have notified at least one national eID means available for their citizens in order to access and use public online services.[13] Additionally, in many countries, public eID schemes under eIDAS are not available for use by the private sector.

2. In Member States where a public and accessible eID scheme is available, **not all relevant registration data fields can be verified by eID**. For example, eID can verify the identity (name) of a domain name holder, but not their contact details.

3. **eIDs are not generally available for verification checks of registration data provided by legal entities**. There is no formal way to do verification checks on legal entities to the same level of accuracy as with regards to private persons. Global legal entity identifiers (LEI) are accepted as an optional attribute in national eID infrastructure.[14] However, there are numerous other obstacles for a wider adoption of LEI, including costs for registering and maintaining them within LEI issuing institutions.[15]

4. **Challenges for the cross-border use of eIDs for registration data verification**. Even if national eID schemes exist, they are not necessarily easy or available for cross-border use.

---

12 Recital 61 of the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 ('NIS 2 Directive'), 4-column table, 17 June 2022.

13 See country overview maintained by the European Commission here: https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Country+overview

14 Response of the Global Legal Entity Identifier Foundation (GLEIF) to the European Commission on the Report on the Application of the eIDAS Regulation Evaluation Roadmap, October 2019.

15 Financial Stability Board, "Options to Improve Adoption of the LEI, in Particular for Use in Cross-border Payments", 7 July 2022.

5. **Inability to use eID verification for non-EEA registrants**. The domain name space is essentially global, and several European ccTLDs offer their services to registrants outside the EU. While eIDs could be used for the partial verification of registration data of nationals of the respective Member State where the ccTLD is established (if an eID scheme is available), and in exceptional cases cross-border within the EU, there is no equivalent eID verification method for registrants outside of EU. The lack of eID solutions for verifying registrants outside of a national territory makes identity checks resource-intensive.

Some of the above-mentioned challenges could be addressed by the revision of the eIDAS Regulation that may open the eIDAS infrastructure to use by private businesses. The European Commission proposed eIDAS 2.0 in 2021.[16] However, any potential positive impact of eIDAS 2.0 is not something that registries may expect in the near future, as the negotiations on the new law are still ongoing, and the intricacies of an EU-wide eID scheme will be left for the subsequent implementation phase, once the law is finalised. Meanwhile, the RegeID project, as initiated by .cz, .nl, .ee and .dk was aimed at ccTLD registries to offer cross-border identification and validation services to EU registrants, which is based on the existing eIDAS infrastructure already provided in these four countries.

However, the updated and improved eIDAS infrastructure will not alleviate the burden of verifying non-EEA registrants. In this case, a risk-based approach can be generally considered to be more proportionate, rather than a blanket and general verification requirement targeted at *all* registrants.

Methods including payment and financial data

As evident above, only a few registries make use of payment and financial data to offer an additional level of verification for registration data, in the absence of national eID solutions or as an additional vector for increased accuracy. It is important to note here that verifying against payment and financial data is most often a manual process that requires human intervention. As a result, this verification method is not scalable. Registrars are most commonly the provider that has that direct contact with registrants, including handling payment and financial data, and this type of verification method relies on cooperation with the relevant registrar. Similarly to the above-mentioned limitations with eID verification, verification via payment and financial data does not offer a solution for full compliance with the NIS 2 Directive requirement, as contact details are out of the scope of such verification.

The Estonian Internet Foundation (.ee) relies on national eID solutions to verify the identity of .ee registrants, in addition to requiring registrants to pay for the applied domain name via bank transfer from a bank account opened in the name of the registrant or the registrant's representative, or from a verified PayPal account registered in the name of the registrant or their representative.

EURid (.eu) conducts 'Know-Your-Customer' checks that require .eu domain name holders to provide evidence of their identity. They can do so either via a scan of the machine read-

16 Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM/2021/281 final, June 2021.

able zone (MRZ) of their passport and SMS, Belgian electronic eID, or via a bank transfer if 1) the domain name holder's bank account has the same name and address as the domain name and if 2) the bank account is in the European Union, Iceland, Liechtenstein or Norway.

DNS Belgium (.be) conducts verification checks via eID methods, including the use of external identity verification service providers such as Itsme and Onfido.

Verification of foreign registrants

The majority of European ccTLDs do not limit their registration eligibility criteria to residents of their country, meaning that domain names within their ccTLD are also available for registration for registrants across the EEA and also outside of the EU. Automated and reliable verification of foreign registrants remains a challenge. Some of the notable practices across European ccTLDs are as follows:

DK Hostmaster (.dk) subjects all registrants who are not resident in Denmark to an automated risk assessment that evaluates the estimated level of accuracy of their registration data. In cases of high-risk registrations (i.e. the level of accuracy is assessed to be low), domain names are delayed from being delegated and the registry requires proof of identity from the registrant. In cases of low-risk registrations, registrants have up to 30 days after registration to provide proof of identity, while their domain name is delegated and can be used. No-risk customers are not required to provide proof of identity.

ICI (.ro) requires foreign registrants to submit a scanned copy of their ID in order to verify that it corresponds to the information provided upon registration.

CZ.NIC (.cz) requires domain name holders outside of the EU/EEA to provide a valid contact address within the EU/EEA upon request, or to designate a representative with an email address within the EU/EEA at which the holder may receive emails related to its domain names.

SIDN (.nl) may occasionally resort to the help of the Royal Netherlands Marechaussee to check the validity of foreign IDs.

Putting in place a reliable source of verification for non-EEA residents remains a challenge. Several registries require the submission of scanned copies of passports and other official ID documents. However, some Member States limit the requirement to request official ID information[17], which makes it challenging for a registry to ensure the accuracy of registration data in the absence of other more reliable methods. The reliability of online copies of photo IDs also poses a challenge, as stolen IDs can be repurposed by malicious actors for instance to pass video ID checks.[18]

In addition, the requirement to submit copies of ID documentation that are then manually checked by an employee is considered to be resource-intensive, error-prone and not cost efficient, since there is no forensic expertise that can be expected from technical operators, such as ccTLDs.

17 See for example the advice of the President of the Personal Data Protection Office (UODO) to banks in Poland: "Making a copy of ID documents is legal only if it results directly from the statutory provisions", 17 September 2019.

18 ENISA, "Remote identity proofing: attacks & countermeasures", 2022.

Contact details validation and verification

The most common way of validating the contact details of registrants are the syntax checks (i.e. the email is provided in a correct format, phone number is provided with a valid country-code and within the character limit) and reachability checks via e-mail or an SMS (i.e. the registrant can be reached via the provided email address and/or phone number). These checks also enable the registrant to provide more details if necessary for further *verification*, i.e. provide other required documentation via email. Syntax checks can be performed automatically, while reachability checks may require human resources. One of the ways to minimise the efforts of validating the reachability of emails is to use bounce checkers.

Hereby, it is worth pointing out that the *verification* of contact details is challenging. If in some cases the accurate and most up-to-date postal address could be verified by requiring the submission of utility bills or sending registered letters to the indicated postal address, for email addresses and phone numbers it is virtually impossible to *verify* if they belong to the person that claims to be the registrant. A simple online search for 'phone number verification' yields numerous results of providers offering disposable virtual phone numbers for required verification for the use of online services.

CZ.NIC uses external service providers to validate the contact details of both local and foreign registrants. For postal addresses, CZ.NIC sends letters via OPTYS, and for phone number validation they use a regional SMS provider ProfiSMS.

DK Hostmaster conducts phone number verification in the event of a notification that the provided number is not correct. Verification checks are conducted by a lookup in the yellow pages, matching the country code of the number with the postal address, or by calling the number.

The role of registrars

Based on CENTR data in the context of registrant data collection, the majority of registries consider themselves to be the data controller in their relationship with registrars. Another common arrangement with registrars within European ccTLDs includes a mixed role of both data controller and processor depending on the dataset. The vast majority of those registries that consider themselves to be the sole data controllers provide instructions on what registrars collect and transmit via the registry-registrar agreement.

In the context of data accuracy, it is generally considered to be the registrar's responsibility to collect and hand over all necessary registration data to registries, including putting in place relevant validation and verification procedures. Registries generally do not provide any requirements for the methods and means that registrars may choose to fulfill their obligation under the registry-registrar agreement.

No specific sanctions are generally envisaged for a registrar's violation of accuracy provisions. In some exceptional and systematic cases of contract infringements, the registrar accreditation can be revoked but there are no reported cases of such a drastic measure ever being used in the context of accuracy provisions.

The most tangible outcome of inaccurate registration data is the revocation of a domain name registration, as essentially it is the responsibility of a registrant to provide registries and registrars with accurate identity and contact details.

The NIS 2 Directive includes a provision to avoid the duplication of accuracy efforts between registries and registrars. As a result, registries and registrars should cooperate to avoid the duplication of the *collection and maintenance* of registration data in order to comply with Article 23[emphasis added].

Since registrant identification data is personal data, in the relationship with registrars and other entities providing registration services, the most common arrangement is the controller-processor agreement across the European ccTLD space. This means that registries are usually in charge of instructing registrars as to which data needs to be collected and transmitted. It is unclear how the NIS 2 requirements will impact existing controller-processor agreements in place across the EU domain name space. It might be worth clarifying at national level within the implementation phase that the purpose of the NIS 2 clarification on avoiding the duplication of the collection and maintenance of registration data should only concern the verification obligation to alleviate the burden on domain holders to provide additional identification information to multiple entities.

At the same time registries and entities providing registration services, such as registrars, should be able to have the flexibility to divide the burden of the data accuracy obligation under the NIS 2 Directive to allow different arrangements across the EU domain name space, accommodating national specificities, the availability of tools and the size of providers.

In addition, considering national specificities, it is desirable to allow flexibility for registries and registrars in choosing the verification methods, as technological solutions are changing quickly. For these reasons, the NIS 2 Directive's implementation and any revision of national rules should stay technologically neutral and not prescribe any methods on how to comply with accuracy-related provisions, in the interest of future-proof policymaking.

> Internetstiftelsen (.se) is working on a voluntary program with registrars who can implement an eID check and share the needed identification data with the registry via EPP, without the need for the registry to duplicate the efforts. One of the biggest Swedish registrars, Loopia, has already implemented eID login for registrants.
>
> CZ.NIC (.cz) requires registrars to make reasonable efforts to verify data before handing it over to the registry and provides the tools for registrars to conduct contact information validation, such as MojeID, which is a Czech eID enabling citizens to prove their identity online and which allows them to log into private and public services.

Proxy services

Historically, the use of privacy and proxy services were intended to protect the identity of registrants and to prevent their personal data from becoming publicly available via WHOIS, a directory service maintained by the registry where information about the registrant and contacts for technical and administrative issues related to a domain name can be queried. However, this has become less of a concern after changes by registries in response to the EU

GDPR. Notwithstanding, there remains a growing proliferation of privacy and proxy services within the domain marketplace which raise several significant issues under existing law as well as potential obligations contained in the proposed NIS 2 Directive.

A privacy service is a service provided by a third party that prevents certain contact information for a registrant from appearing in registration directory services such as WHOIS. A privacy service allows a registrant to appear as the domain name holder of record, but it provides alternate contact information for that registrant. For example, the privacy address might provide a forwarding address in place of the registrant's home address.

A proxy service is a service provided by a third party that shields the identity of a customer by becoming the domain name's holder of record. When the domain name is queried via WHOIS, the identity and contact information for the proxy service is shown.

All validation processes and most verification processes would fail to catch the obfuscation of the real identity of the registrant when a privacy or proxy service is being used. The data provided by the privacy or proxy service could still pass the validation and syntax checks and even reachability checks.

As proxy services are also included under the definition of entities providing registration services that are responsible for data accuracy obligations with regard to registration data under the NIS 2 Directive, it might be worth clarifying at national level that in the event that access to the real identity of a registrant is needed, legitimate access seekers should request that information from the proxy provider.

Conclusions

The current data verification processes in European ccTLDs are evolving and balance data protection requirements with an increasing pressure to identify registrants. The introduction of publicly available eID systems in some Member States has provided a substantial improvement for the identification of registrants that are residents in those countries. However, many Member States have yet to put in place their own eID scheme, and the verification of non-EU residents remains an issue. The roll-out of more public eID systems and the reinvigorated eIDAS Regulation could provide additional tools to introduce increased registrant data accuracy across the EU.

European ccTLDs only collect that data which is necessary to allow the maintenance of a robust and stable internet infrastructure service. Some ccTLDs also process that data in a way that helps them ensure a safe and secure zone. They differ widely in business model, organisation size, local legal policies and requirements, and terms and conditions, which means that a one-size-fits-all approach to data accuracy would not be an effective solution. On the contrary, European ccTLDs are widely recognised to provide the best practices in the industry, and the diversity in their data validation and verification practices and policies, has proven to be a structural strength in the European DNS space as it avoids single points of failure and creates a marketplace of ideas that encourages innovation.

ANNEXES

ANNEX I: Data referenced in NIS 2 as collected by EU ccTLDs on 8/9/2022

ID	Country	Natural person			Legal entity		
		Registrant full name	Email	Phone	Org name	Email	Phone
.at	Austria	Y	Y	N	Y	Y	N
.be	Belgium	Y	Y	Y	Y	Y	Y
.cz	Czech Republic	Y	Y	Y	Y	Y	Y
.de	Germany	Y	Y	N	Y	Y	N
.dk	Denmark	Y	Y	Y	Y	Y	Y
.ee	Estonia	Y	Y	Y	Y	Y	Y
.es	Spain	Y	Y	Y	Y	Y	Y
.eu	European Union	Y	Y	Y	Y	Y	Y
.fi	Finland	Y	Y	Y	Y	Y	Y
.fr	France	Y	Y	Y	Y	Y	Y
.gr	Greece	Y	Y	Y	Y	Y	Y
.hr	Croatia	Y	Y	Y	Y	Y	Y
.hu	Hungary	Y	Y	Y	Y	Y	Y
.ie	Ireland	Y	Y	Y	Y	Y	Y
.it	Italy	Y	Y	Y	Y	Y	Y
.lt	Lithuania	Y	Y	Y	Y	Y	Y
.lu	Luxembourg	Y	Y	Y	Y	Y	Y
.lv	Latvia	Y	Y	Y	Y	Y	Y
.mt	Malta	Y	Y	Y	Y	Y	Y
.nl	Netherlands	Y	Y	Y	Y	Y	Y
.pl	Poland	Y	Y	N	Y	Y	N
.pt	Portugal	Y	Y	Y	Y	Y	Y
.ro	Romania	Y	Y	Y	Y	Y	Y
.se	Sweden	Y	Y	Y	Y	Y	Y
.si	Slovenia	Y	Y	Y	Y	Y	Y
.sk	Slovakia	Y	Y	Y	Y	Y	Y

Council of European National Top-Level Domain Registries

About CENTR

CENTR is the association of European country code top-level domain (ccTLD) registries, such as .de for Germany or .si for Slovenia. CENTR currently counts 52 full and 9 associate members – together, they are responsible for over 80% of all registered domain names worldwide.

The objectives of CENTR are to promote and participate in the development of high standards and best practices among ccTLD registries.

Full membership is open to organisations, corporate bodies or individuals that operate a country code top-level domain registry.

CONTACT

CENTR VZW/ASBL
Belliardstraat 20
1040 Brussels, Belgium
0885.419.166 | RPR Brussels

+32 2 627 5550

secretariat@centr.org

www.centr.org

FOLLOW US

To keep up-to-date with CENTR activities and reports, follow us on Twitter or LinkedIn

Publication date: 11 October 2022