NIS2

WORKSHOP REPORT

NIS2 Directive –
The Impact on the DNS Industry

Minutes of the workshop on Article 28 at ICANN78

in Hamburg, 20 October 2023

MOIN*

*Moin Universal greeting in Hamburg that is used at all times of the day.

eco

ASSOCIATION OF THE INTERNET INDUSTRY

NIS2

WORKSHOP REPORT

Workshop on Article 28 at ICANN78 in Hamburg, 20 October 2023

We thank the sponsors for their support of eco's ICANN78 Accompanying Programme:

CentralNic Registry
geoTLD.group promoting local digital identities
GoDaddy
Google
InterNetX
IONOS
iPHH
nameshield Online Assets Security
.org
RICKERT.LAW WIRTSCHAFT | DIGITAL | RECHT
team internet group plc
VERISIGN

Content

eco – Association of the Internet Industry invited stakeholders in the DNS industry to discuss the impact of the EU's cybersecurity legislation, NIS2, on the domain name industry in the European Union on Friday, 20 October, at a Day Zero Workshop at ICANN78 in Hamburg. The NIS2 Directive is the EU-wide legislation on cybersecurity that may impact not only companies in the EU but also globally. It provides legal measures to increase the overall level of cybersecurity in the EU.

This update of the 2016 NIS Directive broadens the scope of cybersecurity regulation to encompass new sectors and entities, enhancing the resilience of both public and private bodies. Notably, it impacts domain name registrations in the EU, with requirements for domain name registrations specified in **Article 28** of NIS2. The decentralised nature of the directive poses a challenge, potentially resulting in divergent validation procedures across the 27 Member States of the European Union. It came into force in January 2023, and Member States have until October 2024 to transpose the directive into national law. Businesses must assess the directive's applicability and its implications at the technical, operational and legal level. Additionally, agreements need to be entered into with partners as Art. 28 of NIS 2 addresses registries, registrars, resellers and privacy and proxy service providers. Top of Form

Thomas Rickert, Director Names & Numbers, **eco – Association of the Internet Industry**, moderated the full-day workshop at the Hamburg Conference Centre with around 125 participants, with a further 20 participants who joined online. He noted that, when comparing NIS1 to NIS2, there is one outlier, **Article 28** , that has been the source of much debate and contention. Like it or not, he stressed, "We are all on Team 28 now, and we have to make it work one way or the other". There are many different stakeholders at this event, representing both the regulatory side as well as the implementing side. He called on everyone to try to come up with measured responses to the regulatory challenge of NIS2 in order to avoid fragmentation as much as possible, not only within the gTLD space but also between the gTLD and the ccTLD spaces.

He urged all parties to try to maintain a user-friendly experience in the registration and use of domain names to make it easier for those who are the end users. And to avoid the duplication of effort up and down the value chain and to build as much as possible on existing approaches.

1. Introduction to NIS2 and Article 28 – Requirements & Expectations

National legislative bodies are already working on draft legislation to implement the NIS2 Directive in their respective countries. **Juuso Järviniemi**, Policy Officer, Cybersecurity & Digital Privacy Policy, **European Commission, DG CNECT**, kicked off the workshop with an overview of the requirements of the NIS2 Directive, with a focus on Article 28 and the objectives and intentions behind it.

The NIS2 Directive, effective from 2023 and to be transposed into national law by October 2024, introduces measures such as cybersecurity frameworks, national strategies, incident response teams, and risk management protocols. The Directive applies to various entities, including providers of domain name registration services (registrars and also resellers), TLD name registries, and DNS service providers. It excludes operators of root name servers. DNS service providers and TLD name registries are qualified as essential entities regardless of their size.

It sets out specific security requirements, incident reporting obligations and the need for a minimum set of security protocols. It also emphasises the importance of harmonised incident reporting for critical and important facilities, with three stages. The idea is to ensure that you first provide quick information about the incidents (within 24 hours) and then more information in an incident report within 72 hours, but then you have time to actually deal with the incidents. A final detailed report must be submitted within one month of the incident.

Implementing acts will address cross-border issues, focusing on technical requirements and incidents. ENISA will be tasked with managing a registry of entities and collecting relevant information for competent authorities, such as entity details, addresses and the services provided. Information on IP ranges is to be included but not forwarded to ENISA.

The jurisdiction and territoriality guidelines define the scope of jurisdiction for entities. Jurisdiction is exercised by the Member State where the entity has its main establishment, i.e., where decisions on cybersecurity risk management are predominantly taken. Non-EU entities offering services in the EU must designate a representative (a natural or legal person) in a Member State where they operate and are then subject to the jurisdiction of that State.

Questions & Answers:

Michele Neylon, CEO, **Blacknight**, an Irish hosting provider and registrar, asked about the IP ranges; are they for the entire network, or only for the DNS or for other specific services? He pointed out that this is potentially a huge number of IPS, which may or may not be of any relevance. Juusu answered that the Directive stipulates that Member States should require entities to submit at least the IP ranges (which will not be forwarded to ENISA; Art. 27 (4)) and telephone numbers of the entity (**Art. 27 (2)(f)**) and invited Michele to contact him by email to get more information on the exact IP range required.

Both **Michael Palage**, Chief Trust Officer, **InfoNetworks**, and **Amadeu Abril i Abril, COREhub**, asked about whether resellers are included in **Article 21 (2)(d)**, which addresses supply chain security, including security-related aspects of the relationship between each entity and its direct suppliers or service providers, and any obligations for resellers. This is still under discussion, responded Juuso, and will be addressed in the implementing acts that will be drafted once all Member States have provided their input to the Commission.

Gemma Carolillo, Deputy Head of Unit, Next Generation Internet, **European Commission, DG CNECT**, continued the introduction to Article 28, pointing out that while much attention is currently being paid to this one article, the whole Directive is very much relevant for the DNS sector. The DNS is given an important role in the NIS2 Directive, which recognises its critical role:

> "upholding and preserving a reliable, resilient and secure DNS are key factors in maintaining the integrity of the Internet and are essential for its continuous and stable operation, on which the digital economy and society depend."

The importance of domain name registration data (so-called 'WHOIS data') is recognised, and the availability and accessibility of the data is linked to the prevention, detection and response to DNS abuse. The main objectives of Article 28 are to contribute to enhancing the security, stability and resilience of the DNS, thereby strengthening cybersecurity in the Union. It aims to establish a legal framework that guarantees the accuracy, completeness and accessibility of domain name registration data to legitimate access seekers. While providing for a set of obligations to achieve these objectives, the Article refrains from specifying a particular implementation model, instead encouraging the use of existing and evolving best practices.

Carolillo highlighted several points for consideration in relation to the obligations to collect domain name registration data. Article 28 establishes a clear legal basis for TLD registries and entities providing registration services to process data for a specific purpose, as a legal obligation (**Article 6(1)(c) GDPR**). This obligation does not limit the possibility of collecting domain name registration data for other purposes, such as through contractual agreements or legal requirements set out in other Union or national legislation (**Recital 109**).

Entities can and must process the registration data as this is a legal requirement. In addition, these entities must have policies in place to ensure the accuracy of the data, and these policies must be made publicly available, including the verification procedures used. In addition, entities are required to publish non-personal data, such as legal entity information, without undue delay. They must provide access to certain personal data upon a duly substantiated request from a legitimate access seeker and ensure that all access requests are responded to within 72 hours.

She also pointed out that NIS2 recognises that the DNS is a distributed system where cooperation is required to achieve its objectives. Recital 109 states that TLD name registries and entities providing domain name registration services should cooperate to avoid duplication in the collection of data from registrants.

2. Report from the NIS Cooperation Group

Finn Petersen, Director of International ICT Relations, Division for Digital Regulation and Supervision, **Danish Business Authority**, is the Danish representative on the Governmental Advisory Committee (GAC) and, in the NIS Cooperation Group, also the Chair of the WS for Digital Infrastructure and Providers and the WS on WHOIS. He stressed that NIS2 and Article 28 on WHOIS will not be covered by an implementing act. It will be up to the Member States to implement it. The purpose of the WS on WHOIS is to provide guidance on Article 28 in order to have a harmonised approach to the implementation and application of the provisions of the Article at the national level in order to avoid too much fragmentation of the market. This is perhaps the most difficult paragraph in this legislation to implement, in his view. He thinks that they won't come up with just one method, but there might be a limited method that the NIS Cooperation Group will recommend to Member States.

The main objective of the Task Force on Verification is to develop draft guidelines covering the provisions in **Article 28(1)-(4)**, e.g. methods for verifying WHOIS data, how and when to verify WHOIS data already collected, etc. The Task Force on Legitimate Access shall develop draft guidelines covering the provisions of Article 28(5), e.g., criteria for legitimate requests, what should be delivered within 72 hours, how to deal with an urgent request, whether there should be a system or form to be used by the applicant, etc.

Questions & Answers:

Barbara Povse, head, **Register.si**, wanted to know how to find out who is participating in the NIS2 Cooperation Group from different countries. Finn recommended contacting the national government and the respective national representative in the Cooperation Group.

Bart Mortelmans, owner, **bNamed**, asked which regulations apply if, for example, a French person buys a Danish domain name from a registrar in Belgium. Could this harm competition between registrars in different countries or create back doors that would allow people to circumvent validation procedures? **Petersen** referred to the principle of jurisdiction that **Järviniemi** of the European Commission explained earlier: Jurisdiction is exercised by the Member State where the entity has its main establishment, i.e. where decisions on cybersecurity risk management are predominantly taken.

Neal McPherson, Head of Product Management Domains, **IONOS**, asked whether some Member States had indicated that they were waiting for guidance from the Working Group before moving forward with their own individual legislation, or whether they were working in parallel and possibly independently of the NIS2 Cooperation Group. Petersen replied that a meeting in mid-November will provide clarity on how Member States are proceeding. He mentioned two approaches that Member States could take. One option is to transpose the Directive into national law and then follow up later with an implementing regulation or secondary legislation incorporating the guidelines. Another option, depending on the legal tradition, would be to include in the implementing legislation a note stating that the guidelines developed by the NIS2 Cooperation Group or the European Commission, etc. should be taken into account for certain paragraphs.

Ashley Heineman, Chair of the Registrar Stakeholder Group at ICANN (RrSG), as well as **GoDaddy**'s Director of Global Policy (attending the workshop and speaking on behalf of the RrSG), offered to share with the NIS2 Cooperation Group how they operate and do things as a large registrar with a range of different business models and practices. There is a lot of work that needs to be done, for example, their contracts with ICANN. They are happy to be a resource and share best practice, so that this does not have to be duplicated.

3. National-level deliberations on Article 28

NIS2 must be transposed into national law by national legislators by 17 October 2024 and will apply from 18 October 2024. As a result, proposals for national legislation are already in the pipeline. Four speakers analysed and discussed selected draft proposals from their respective EU Member States to provide insights into the national legislative processes and implementation of legislation.

Dirk Jumpertz, Security Officer, **EURid**, reported that EURid falls under the Belgian legislation. He found the interaction with the Belgian regulator to be quite fruitful over the last few years. They have consistently shown openness in trying to understand how EURid works, including during the transposition process for the NIS2 Directive.

Sophie Kreizer, Ministry of Economic Affairs and Climate Policy, The Netherlands, explained the different perspectives they have to take into account with the different ministries involved in implementing the NIS2 Directive, like Economic Affairs (feasibility of verification processes, best practices) and Justice and Safety (investigation, unwanted content). The Ministry of Economic Affairs and Climate Policy is committed to working with the sector and best practices and is represented in the NIS2 Cooperation Group workstreams. They are learning from the Dutch registrar and registries about best practices in the community, such as email verification (before a domain can be made available), and are looking at including these in Dutch legislation. The goal of the Dutch government is to achieve a minimum of harmonisation within the EU and, hopefully, within the ICANN community.

Jaromír Talíř, Technical Fellow, **CZ.NIC**, provided an overview of the Czech government's implementation of the NIS2 Directive. The National Cyber and Information Security Agency has been in charge of the implementation process and the revision of the Czech Cybersecurity Act of 2014. A draft was already published in January 2023, and public comments and feedback have been taken into account in the second draft, which is currently being revised following feedback from government agencies. It is expected that the government will vote on it at the end of 2023 and that the legislative process in Parliament can start in 2024.

Article 28 of the Czech draft is largely copied from the NIS2 Directive, with the main change being to grant access to the national eID database to both TLD name registries and entities providing domain name registration services. Currently, this access is only allowed to entities with a legal obligation to verify identities. Paragraph 6 was originally moved to an explanatory note but was reinserted into the legislative text after Czech intervention. There is significant opposition from some lobby groups in relation to supply chain security. If this continues, then it could delay the whole implementation of NIS2, which could have an impact on the Czech elections in 2025.

Peter Vergote, Legal & Corp. Affairs Manager, **DNS Belgium**, echoed **Jumpertz**'s view that there is a stable and cooperative contact between the registrars and the regulatory authorities, in particular the Belgian Institute for Post and Telecommunications.

The system for verifying registration data was already in place in Belgium before they became aware of NIS2. One challenge is to align what is already in place in Belgium with the requirements of NIS2, with the hope that they don't have to start from scratch and completely rebuild the registration and verification system. **Carolillo, European Commission**, later commented in response that if there is a system in place which is compliant with the Directive, it does not need to be changed.

The Belgian ccTLD has gained useful experience in verifying registrants, e.g. what to do if verification fails; will the domain be lost or kept (as the registration fee has already been paid)? The Belgian experience here could be useful for the implementation of NIS2 in the coming years.

3.1 Issues in dealing with national lawmakers

The four speakers also addressed the main issues that have been identified, either legal or technical, in their deliberations with the national lawmakers. Speaking for the Netherlands, **Kreizer**, referred to the question raised earlier by **Mortelmans, bNamed**. One of the challenges faced is the lack of clarity on certain issues. For example, consider a scenario where a Dutch individual wants to register a German domain name through an Irish company. In such cases, it is still unclear which jurisdiction applies. This complexity highlights the necessity of the European workstream groups, where the industry and lawmakers can collaboratively establish policies and agreements to address such concerns.

Regarding **the scope of necessary verifications, Jumpertz, EURid**, reported that they have extensively debated the extent of these verifications. Initially, the Belgian regulator proposed verifying all registrations, but the operational burden of this approach became a prominent concern, amounting to 7 verifications per minute, 365 days of the year: a gigantic operational load. As a result, EURid has shifted its focus to discussing new registrations and associated risk assessments. Defining these assessments and the criteria they're based on remains a significant challenge.

From the Czech perspective, J**aromír Talíř**, **CZ.NIC**, said that the most significant challenge during this dialogue was **the need to explain to the government** why they were seeking certain capabilities. For example, when he brought up the issue of access to the national eID database, the initial response was dismissive, suggesting it wasn't a matter of concern because TLD name registries and entities providing domain name registration services were allowed to access it. However, he had to clarify that they did not actually have permission to access this data. He had to facilitate communication among different government entities to ensure this capability was included.

Vergote, DNS Belgium, highlighted the concern of **regulatory shopping** as a significant issue in the context of Article 28. He emphasised the potential for Member States to implement varying degrees of validation requirements for the opaque data mentioned in the Article, such as email, telephone numbers, and registrant names. This could result in different approaches to validation, from a simple email validation to a comprehensive verification process involving multiple data points. He warns that such an uneven regulatory landscape could lead to, e.g., non-EU registries that have to choose a representative in the EU opting for one based in the country with the least stringent regulations, and so possibly distorting competition. To address this, he suggests the need for a unified approach to prevent regulatory discrepancies and ensure fair competition.Bottom of Form

In response, **Gemma Carolillo, European Commission**, pointed out that Member States can choose to impose stricter regulations, but it seems unlikely that they would interpret the paragraphs creatively, leading to the imposition of different rules. The primary objective of the NIS2 Cooperation Group is to ensure the **broadest possible harmonisation**, thereby fostering compliance across systems. While it's essential to acknowledge this possibility, it's reasonable to assume that most national governments aim for consistency rather than introducing different systems.

Johannes Loxen, CEO, **SerNet**, later emphasised the challenge of legislative variations, citing the example of the difficulty of translating specific terminologies in legal texts, complicating the understanding of regulatory requirements. He highlighted the need for meticulous analysis of multiple legislative frameworks, underscoring the complexity of navigating diverse jurisdictional policies.

Questions & Answers:

Amadeu Abril i Abril, COREhub, asked at **what level the verification process should be anchored**. The verification process should be at a single level; otherwise it won't be effective. For example, at COREhub, a registrar that only works through resellers, they've implemented email verification and offer their members two options. They can either customise an email with their logo and name for verification through their system, or they can send them a copy independently. Without this centralised process, if they, as the registrar, initiate the verification, the registrant may mistake it for spam due to the lack of a direct commercial relationship. Therefore, it's critical that this verification process is not fragmented across multiple levels but is handled by the party that has the commercial relationship with the registrant.

CoreHub has members who are Dutch and act as registrars for .nl, but also serve as resellers for, e.g. ICANN. They have resellers in various EU countries. Their current verification system can handle different systems for different TLDs, as well as individual ccTLDs. Technically, he finds it challenging to envision how the verification process for a Dutch member's .com differs from that of a German member, or how the registrant's location in Sweden affects it. Building a system that manages these verifications, conducts checks, and enforces consequences within varying timeframes, ranging from 15 to 21 days, while ensuring consistent treatment of the same entity, appears impossible.

He strongly urged that this verification should be done only once per domain and that the obligation to verify should be at the registry and registrar level, not at the reseller level.

On the topic of resellers, **Carolillo, European Commission**, reminded the participants that **resellers are explicitly included** in the definition of entities providing domain name registration data. Consequently, this impacts supply chain risks, particularly where the DNS service provider is working with a reseller. The specifics regarding this inclusion in the security measures section of the Implementing Act are currently under preparation, and no information is yet available. While the existing distributed system is expected to remain unchanged, the procedure applied needs to be transparent, which will require the publication of the process to ensure that it isn't shrouded in secrecy. This clarity is crucial for supervisory authorities to effectively monitor compliance.

Chris Disspain, Identity Digital, asked what to do with a registrar that has a contract with a ccTLD outside of Europe, which is governed by the law of the country in which that ccTLD is based. How should such registries and registrars be dealt with?

In terms of territoriality, **Carolillo, European Commission**, explained the debate is primarily about service provision within Europe. This distinction means that **if a registrar does not provide services to the EU, it is outside the scope of the Directive**. ENISA's ongoing work to establish a registry of entities is expected to provide further clarity on this issue. It is either the establishment of the entity or the provision of the service that determines whether it falls within the scope of the Directive. The ultimate service is the registration of the data. Therefore, it's not possible to include the registry in the scope and exclude the registrar, or vice versa, especially when discussing the registration of EU-related data. The whole operational chain has to be considered. Viewed from this perspective, there must be an (EU) registry if the registrar is registering in the EU.

Bruce Tonkin, Chief Operating Officer, .**au Domain Administration**, asked whether there's a distinction regarding whether **the name of an individual involved in business activities is considered non-personal data** or if the right to privacy always applies, especially when comparing individuals with corporate structures. In Australia, individuals conducting business or engaging in trade are considered to be legal entities.

Carolillo, European Commission, explained there's a clear focus on legal entities within the Directive, particularly with the requirement for publication of non-personal data. The Directive specifically mentions the need for publication of legal entities and registrant names. There's also a specific focus on the use of contact email, emphasising the importance of avoiding the disclosure of personal data. This means that when referring to legal entities, alternative approaches, such as the use of a pseudonym or other means of hiding personal data, could be used, ensuring that the registered name of the organisation remains visible.

3.2 Disruptions to the domain name life cycle

There have been discussions at the national level regarding potential systems that might disrupt the conventional domain name lifecycle. Some ideas have been proposed, such as the suspension of domain names, preventing their delegation until specific procedural steps have been completed.

Dirk Jumpertz, EURid, gave an example. There are specific requirements for .eu domain registrations, all falling under the eligibility criteria, meaning that not everyone can register a .eu domain. They follow distinct rules that are enforced by mechanisms **that separate the registration process from the delegation process**. Registration involves the administrative purchase of the domain, while delegation includes adding the domain to the zone file to make it functional. An abuse prevention system acts as an intermediary, intervening in the event of eligibility issues or other concerns, enabling an early warning system to trigger data verification during new registrations. If registrant data cannot be verified, the domain will not be delegated. Although this approach isn't common in the industry, it has proven effective in various cases, including law enforcement and botnet removal, as well as verifying legitimate domain name registrations during the Covid-19 pandemic.

A significant challenge here is that registrants receive messages from unfamiliar entities, specifically the registry responsible for a particular top-level domain. This poses a considerable hurdle in confirming the registrant's identity, often conducted via email, which is widely recognised as an unreliable method of communication. Establishing trust in these email verifications is a key concern, as some entities fail to respond to verification requests, resulting in domain suspensions that can be disruptive, particularly on a global scale.

Peter Vergote, DNS Belgium, spoke about a new status they have introduced for domain name registrations. The implementation of this measure raises questions about the consequences of failed verifications. In cases where a registrant is unable to provide sufficient evidence for data verification, strict revocation of the registration could entail significant financial implications, necessitating reimbursements for both the registrar and the registrant. Alternatively, it may be more practical to allow the registrant to retain the domain name title but prevent its functional use, aligning with cybersecurity objectives to curb potential fraudulent or abusive activities. Our current approach involves **maintaining the inactive status of the domain name until successful verification occurs**, ensuring the registrant's entitlement to the name until the yearly renewal period. This issue gains further complexity when considering historical database entries, where the reluctance to delete a long-standing registration due to verification failure is heightened by various potential factors, such as outdated contact information. Therefore, the implications of these measures should be carefully considered within the context of implementing Article 28.

4. Multistakeholder organisations

The language of NIS2 refers to multi-stakeholder organisations. **Elena Plexida**, Vice President, Government and IGO Engagement, **ICANN**, looked at the interplay between national/regional legislation and the global multistakeholder model, including ICANN, where community policies are already in place.

NIS2 requires that registries and entities providing domain name administration services establish policies and procedures to collect and maintain registration data and to disclose them, etc. The NIS2 recitals state that these policies and procedures should take into account "to the extent possible" the standards developed by the multi-stakeholder governance structure at the international level; so ICANN. The EU itself emphasised the multi-stakeholder model is best suited to ensuring that no one actor is dominant or takes all responsibility for the future development of the Internet. The successful IANA stewardship transition to ICANN in 2016 was highlighted as a positive example of promoting the multi-stakeholder approach. ICANN is the right place to develop policies for the DNS because of its model of optimal, inclusive solutions for the DNS which are globally applied.

Plexida, ICANN, highlighted the importance of the multi-stakeholder model in Internet governance, emphasising the decision-making power and political influence of the DNS community. She emphasised the technical focus of the community, its role in coordinating DNS rules for stability, and its distinct function from legislative processes. While acknowledging the need for legal clarity and GDPR compliance, she cautioned against interfering with multi-stakeholder policy-making through legislative intervention, which could lead to a fragmented regulatory landscape. **Plexida** expressed the hope that the Member States would follow the standards of the ICANN community and avoid conflicting national requirements. She underlined the dynamic nature of ICANN policy and the continuous evolution of the multi-stakeholder model, ultimately advocating its protection in the service of the global Internet.

Questions & Answers:

Steve DelBianco, President & CEO, **NetChoice**, representing the Business Constituency at ICANN, raised a question regarding ICANN's policies and contracts in the context of the European Union and Member States. He inquired whether these policies and contracts must **explicitly stipulate compliance during transposition** or if it is sufficient for ICANN's policies and contracts to provide the contract parties with the flexibility to exceed contractual obligations. He emphasised the need for clarity and flexibility in ICANN's contracts to accommodate various jurisdictional requirements without restricting the contracted parties. Both **Carolillo** and **Plexida** stressed in response that national legislation supersedes ICANN contracts.

Hadia El Miniawi, AFRALO Incoming Chair, believes that ICANN's authority lies in its ability to ensure consistent compliance with laws and regulations across the community and its stakeholders. Using the implementation of the GDPR as an example, she highlighted the shift away from the WHOIS model to address privacy concerns. She emphasised the collaborative efforts within the community to ensure consistent compliance with the GDPR and other relevant regulations for the benefit of users, particularly registrants. Hadia emphasised the importance of harmonising the actions of the contracting parties to avoid individual interpretations and unequal treatment based on geographical location.

Michael Palage, Chief Trust Officer, **InfoNetworks**, asked Elena Plexida to explain the difference between the EU's actions under NIS2 and the Chinese government's real name verification requirements for gTLD registry operators, emphasising **Plexida**'s previous concerns that NIS2 could threaten the multi-stakeholder model.

Plexida, ICANN, clarified, with good humour, that she is not an expert on the Chinese government's actions and stressed that the technical community cannot dictate terms to sovereign governments, whose primary responsibility is to protect their citizens. She reiterated that her previous concerns about NIS2 undermining the multi-stakeholder model were related to the earlier proposal to regulate the server system, which has since been removed from NIS2.

Chris Disspain, Identity Digital, emphasised the sovereignty of each country code top-level domain (ccTLD), whether operated by governments, non-profit organisations or individuals, and that they are governed by their respective countries' laws. As he put it, "If a bunch of those countries choose to come together and operate a federated system of laws. To put it simply, that's entirely a matter for them." He believes that attempts to govern laws for registrants across different ccTLDs will face challenges, as each is subject to the laws of its own jurisdiction. ICANN does not establish policies for ccTLDs.

Thomas Rickert took stock after the previous points, reflecting on the tension between global policies and national regulations in the gTLD world and highlighting the challenge of balancing consistent global approaches with the additional requirements imposed by national jurisdictions such as NIS2. He notes the difficulty of maintaining technical systems that function effectively on a global scale while accommodating differing national regulations. Thomas also pointed to the need to discuss the extent to which ICANN should govern the domain space in relation to national regulators.

5. The role of registration data in the fight against DNS abuse

Recital 110 states that „the availability and timely accessibility of domain name registration data to legitimate access seekers is essential for the prevention and combating of DNS abuse, and for the prevention and detection of and response to incidents." How effective is the use of domain name registration data in combating DNS abuse? What other complementary measures are available?

Brian Cimbolic, Vice President and General Counsel of **Public Interest Registry** (.ORG), described PIR's two main approaches to dealing with DNS abuse: reactive and proactive. The proactive Quality Performance Index (QPI) is an incentive programme for registrars that rewards healthy registration patterns and has resulted in a significant reduction in abuse by approximately 76%. **Cimbolic** emphasised that, from a gTLD perspective, registration data is not essential to effective anti-abuse measures, recognising the differences between ccTLDs and registrars in the gTLD space, where customer information may be more important.

Steinar Grøtterød, Director of Policy & Compliance, **iQ Global AS**, explained that iQ Global offers a set of services to regular operators, registrars, hosting providers, and end users to effectively monitor the namespace for suspicious behaviour, including DNS abuse and other security threats, utilising data from various reputation block list providers. He stressed, "We don't need any personal information." He believes they can support their customers best by providing them with data that is reliable, and proven and that they can pass on to their own customers, who have the information about who can best mitigate abuse.

Volker Greimann, General Counsel and Head of Legal and Policy, CentralNic Group (now **Team Internet**), explains their approach to handling DNS abuse, which is primarily reactive. They receive reports from various sources and scan their database against these reports to identify potentially abusive domains. While they use registration data to identify patterns in registration data provided by perpetrators, they do not directly use personal data for investigating abuse cases.

Chris Lewis-Evans, Director of Governmental Engagement and Internet Abuse Mitigation, **CleanDNS**, was working in law enforcement until recently and brought this perspective to the table. CleanDNS does not generally use registration data as evidence of the abuse it monitors and mitigates. It is usually only used when there are compromised hosts. Then registration data is used to see who to contact. Law enforcement's focus is on protecting victims. They often use registration data to deal with compromised hosts and compromised domains, to contact them and to investigate.

Nick Wenban-Smith, General Counsel, **Nominet UK**, joked to much laughter that, "after five years, we finally see the benefit of Brexit when we look at the NIS2". Nominet UK employs a hands-on approach to identifying abusive activities, using a dedicated compliance team and an algorithm to assess risk factors during the registration process. While they do not block domains outright, suspicious registrations are flagged for further investigation, taking into account various factors beyond just the registration data. The focus is on mitigating risk without impeding the activities of legitimate users. So, while registration data isn't irrelevant, it's just one of a number of factors they look at.

Michele Neylon, Blacknight, raised concerns regarding due process and data access. Specifically, he mentioned concerns that law enforcement agencies might be seeking access to private data without transparency, contradicting the principles of due process. **Lewis-Evans, CleanDNS**, explained that the confidentiality of law enforcement requests is crucial during ongoing investigations to prevent interference. Disclosing such requests could alert the subjects of the investigation, potentially hindering the process. However, once the investigation concludes, transparency about these requests is generally accepted. This approach aligns with the agreement between law enforcement and ICANN.

Michele Neylon, Blacknight, raised further concerns about the complications arising from law enforcement requests for cross-border data access. He cited cases such as Russian law enforcement seeking Ukrainian registry data, Israeli law enforcement seeking Palestinian data, and vice versa, among other potentially challenging scenarios. He emphasised the risks associated with assuming that all law enforcement agencies consistently adhere to legal standards relating to human rights and due process.

Chris Lewis-Evans, CleanDNS, countered that in the UK, for example, registrars have the authority to assess the legitimacy of law enforcement requests and are encouraged to carefully evaluate the purpose behind each request. Data sharing is generally not permitted if it poses a perceived threat to life. He recommended that registrars confronted with such requests should contact their law enforcement authorities in their own country and let them deal with it.

In a discussion initiated by **Thomas Rickert** on the benefits of accurate data, **Volker Greimann, Team Internet**, pointed out that improved registration data alone may not effectively address the problem of DNS abuse, as determined criminals are adept at circumventing such measures. Refining the accuracy of data could eliminate existing flaws and provide one less avenue for identifying fraudulent registrations. **Steinar Grøtterød, iQ Global**, referenced IQ's analysis, emphasising the high prevalence of abuse linked to compromised domains. **Brian Cimbolic, PIR**, clarified the definitions of malicious registrations and compromise domains, highlighting the complexities associated with mitigating abuse without causing collateral damage. **Nick Wenban-Smith, Nominet UK**, expressed scepticism about the necessity of Article 28, citing the robust compliance and data verification practices already in place in several European ccTLDs. **Chris Lewis-Evans, CleanDNS**, emphasised the importance of contract changes for enhancing law enforcement's ability to address abuse. Volker stressed the need for law enforcement empowerment beyond addressing symptoms. **Werner Staub, COREhub**, questioned why bad actors often evade detection despite the vast domain inventory at their disposal, suggesting their strategic manipulation of takedowns. **Michele Neylon, Blacknight**, highlighted the importance of IP addresses in mitigating abuse, emphasising their greater relevance compared to domain names. **Johannes Loxen, SerNet**, urged the GAC to prioritise discussions on addressing professional criminals rather than focusing primarily on easier targets such as music sharers.

The further discussion delved Into the significance of account holder data and its role in investigating perpetrators. **Margie Milam, Meta**, presented a big-platform perspective, underscoring the benefits of accessing WHOIS information to correlate trends and identify larger networks of abuse. **Nick Wenban-Smith, Nominet UK**, emphasised the need for cross-level cooperation, citing the European Internet ccTLD Registry Association's efforts in threat analysis and information sharing. **Michele Neylon, Blacknight**, emphasised the importance of focusing on infrastructure and payment-related issues to combat fraudulent activities. **Steinar Grøtterød, iQ Global**, proposed measures for efficient mitigation, emphasising the need for active monitoring and policy adjustments. **Chris Lewis-Evans, CleanDNS**, stressed the value of comprehensive data sharing and the importance of contract changes in facilitating effective action. Volker highlighted the practical challenges faced by registrars and the significance of using third-party services for detecting abusive domains. **Kristof Tuyteleers, DNS Belgium**, emphasised the need for tech companies to prevent abuse and improve communication among stakeholders. **Brian Cimbolic, PIR**, advocated for capacity-building initiatives and incentivisation programs, urging active participation in the DNS abuse amendments. **Gemma Carolillo, European Commission**, reiterated the lack of a silver bullet solution and expressed support for proactive measures and the broader scope of NIS2 in addressing cybersecurity risks.

6. Operational & implementation challenges

TLD name registries and the entities providing domain name registration services will be required to have policies and procedures in place, including verification procedures, to ensure that databases contain accurate and complete information, to make domain name registration data that is not personal data publicly available, etc.

What are the best practices and challenges in implementing and operating the required policies and procedures, and what are the implications at the national, EU and global levels? Will EU-based companies be at a commercial disadvantage in the future?

Beth Bacon, Senior Director, Policy and Privacy, **Public Interest Registry** (.ORG) / Vice Chair, RySG, emphasised the need for cooperation and collaboration between registries and registrars to ensure smooth operations and avoid duplication of effort. **Samantha Demetriou**, Senior Director – Policy, **Verisign** / Chair, RySG (attending the workshop and speaking on behalf of the RySG), highlighted the restrictions on GTLD registry operators, stressing that they cannot register domains themselves or act as registrars. She stressed the importance of the party closest to the data subject being responsible for data collection and verification.

Ashley Heineman, Director for Global Policy at **GoDaddy** / Chair, RySG, speaking from the registrar's perspective, emphasised the role of the registrar as the entity that interacts directly with registrants, collecting data and maintaining communication with them. She emphasised the need for clarity and consistency in the division of responsibilities and suggested that certain tasks, such as verification, should be streamlined to avoid confusion.

Polina Malaja, Policy Director, **CENTR**, the association of European country code top-level domain name registries, discussed the implications of Article 28 for the ccTLD space, emphasising the challenges of implementation. She highlighted the need to take into account various other pieces of legislation, such as the GDPR, that overlap with NIS2 requirements. **Malaja** emphasised the diversity of data accuracy practices across the ccTLD space, with limited proactive verification checks. She mentioned the lack of electronic identification methods for verifying legal entities, and the ongoing challenges in determining the required level of accuracy for domain registration data. **Malaja** stressed the importance of striking a balance between maintaining domain availability for end users and ensuring high standards of verification to combat DNS abuse. She suggested that while verification is part of the solution, it cannot alone address the problem of abuse in the domain space.

Thomas Rickert raised the issue of sharing responsibilities, noting that some parties suggested the validation task should be with registrars, while others want to do the validation at the registry level. **Polina Malaja, CENTR**, emphasised that registrars are in the best position to communicate with registrants and collect relevant data for verification purposes. She highlighted the importance of allowing flexibility, considering the diverse local requirements and the varying capacities of different registries.

Neal McPherson, Head of Product Management Domains, **IONOS**, representing a larger registrar, supported the view that registrars are well-placed to handle customer communication and data verification, given their direct relationship with customers. He stressed their commitment to maintaining accurate customer data, which is crucial for both financial transactions and ensuring the integrity of registration data.

Thomas Rickert shifted the focus to the issue of data disclosure requests, asking who should handle such requests and at what level - whether it should be the registrar, the registry, the privacy proxy service provider or the reseller. **Michele Neylon, Blacknight**, expressed concern about the challenges that small businesses may face in complying with the regulations, citing the difficulty of managing large amounts of personal information and responding to third-party requests, particularly for businesses with limited resources. He criticised the regulatory landscape, suggesting that it could disadvantage smaller companies and potentially lead to a market dominated by larger companies. **Samantha Demetriou, Verisign**, drew attention to some validated TLDs, such as .bank and .pharmacy, where the registry takes responsibility for validating the registrant outside of the regular domain registration process. **Thomas Rickert** emphasised the need for carefully crafted agreements between the different stakeholders to ensure a harmonised approach while respecting the different needs within the industry.

Pawel Kowalik, Head of Product Management, **DENIC**, emphasised the importance of cooperation between the registry and the registrar level. He highlighted the role of registrars in carrying out verifications and ensuring the accuracy of data accuracy, given their proximity to the market and access to effective tools. Effective tools. He discussed the unique position of many ccTLDs as a national asset, leading to strong interest from local authorities. **Kowalik** highlighted the role of the role in establishing a robust policy framework that enables registrars to carry out reviews effectively without taking over the process from the registries. He advocated flexible verification methods to accommodate different business models, including different payment methods and personalised interactions with registrants. He sees the need to maintain a balance between rigorous verification and the flexibility needed for different registrar operations.

Amadeu Abril I Abril, COREhub, expressed concerns about managing externalities within the ICANN community, highlighting the lack of incentives for responsible behaviour. He suggested considering a reverse application of the "polluter pays" principle, urging that those investing in anti-abuse measures should be the ones rewarded. **Ashley Heinemann, GoDaddy**, countered this by asserting that existing policies, including those outlined in Article 28, are already in place, emphasising the comprehensive data collection and verification processes implemented by ICANN-accredited registrars. **Samantha Demetriou, Verisig**n, discussed the imminent finalisation of the Registration Data Policy and the adoption of the Registration Data Access Protocol (RDAP) in ICANN agreements, noting its advantages over the previous WHOIS protocol. She also emphasised the policy-level cooperation between registries and registrars and its alignment with the principles of Article 28. B**eth Bacon, PIR**, further underscored the flexibility and collaborative nature of the multi-stakeholder model, commending the drafters of Article 28 for recognising the diverse data processing needs and facilitating access to tools for registries.

Alan Woods, General Counsel, **CleanDNS**, emphasised that ICANN does not act as an enforcer of EU law and stressed the importance of allowing contracting parties the freedom to interpret the law in their respective jurisdictions. The Registration Data Policy has been developed to give registries and registrars the legal leeway they need to facilitate compliance without overly prescriptive guidance from ICANN. **Keith Drazek**, Vice President Policy & Government Relations, **Verisign**, provided context on the legal versus natural distinction, referring to his involvement in the multi-stakeholder process within ICANN's EPDP Phase 2a working group. He emphasised the complexity arising from the large number of existing domain registrations that have been collected without distinguishing between legal and natural persons. **Gemma Carolillo, European Commission**, reiterated NIS2's explicit directive to publish legal entity data, including the registrant's name, contact telephone number and email address. She highlighted the Commission's enquiries to the GAC about aligning the publication requirements with the draft Registration Data Policy.

Thomas Rickert highlighted the challenge for registries and registrars to automatically distinguish between legal and natural persons for existing registrations and the additional complexity of determining whether email addresses contain personal data, referring to Article Recital 112. **Gemma Carolillo, European Commission**, emphasised the importance of ICANN's Registration Data Policy and the need to align its provisions with relevant legislation. She emphasised that where actions are optional under the policy but required by other laws, the latter will prevail. Gemma clarified that NIS2 does not seek to replace the Registration Data Policy in its entirety and only covers a small subset of data related to contact information. She stressed the importance of ensuring the accuracy and completeness of the five specified fields.

Michael Palage, InfoNetworks, emphasised the feasibility of making a distinction between natural and legal entities, citing the example of annual accuracy notifications from registrars. He suggested implementing a simple process to identify the type of entity. He also commended the efforts of certain gTLD registries, in particular Verisign, in demonstrating how registrant verification can be enforced in a GDPR-compliant manner.

Ashley Heineman, GoDaddy, expressed frustration over the conflicting requirements of collecting sensitive information for NIS2 while also having to comply with GDPR, emphasising the challenges in ensuring data minimisation and data protection.

Werner Staub, COREhub, underscored the critical nature of the email address in determining the legal entity behind a domain, highlighting the importance of the information that comes after the @-sign in corporate identification, as this is the actual legal entity.

Thomas Rickert asked what considerations IONOS has made regarding contractual arrangements with other parties involved in the sharing of responsibilities. **Neal McPherson** explained the complexities arising from the multiple layers of contractual obligations, including those with ICANN, between registrars and registries, and compliance with local laws that are now becoming more involved in domain registration and management. He foresees challenges as local regulators inquire about verification processes, with potential layers of responsibility shifting between the registry, registrar and reseller.

Chris Disspain, Identity Digital, raised a point about the ambiguity of what constitutes personal information in the context of business details. He questioned whether business-related contact information, such as a personal mobile phone number or a home address used as a business address, should be considered personal information and highlights the need for clear guidelines or consent requirements in cases where the distinction is blurred.

Alan Woods, CleanDNS, was concerned about the clarity of enforcement on a global scale and the potential creation of an uneven playing field. He pointed out that it may be difficult to enforce the rules across all TLDs and ccTLDs, particularly those outside the European Union. He highlighted the impact on SMEs and suggested that the difficulties faced by businesses as a result of these regulations need to be recognised.

Gemma Carolillo, European Commission, explained that the legislative process, including public consultations and multi-stakeholder dialogue, has been transparent and that the legal basis for publication is set out in NIS2, which specifies the purpose of publication of legal entity information. She reiterated that the European Union is open to input and engagement from various stakeholders, including the ICANN community. When asked for clarification on the legal basis for the publication of individual entity information, in particular personal contact details, she affirmed that the legal basis is set out in NIS2 and that the purpose of publication is specified, as required by the GPDR.

6.1 The contractual arrangements between various parties involved in the domain registration process

Thomas Rickert highlighted the importance of establishing clear contractual arrangements between the various parties involved in the domain registration process, including registries, registrars, resellers, and privacy and proxy service providers. He emphasised the need for delineating responsibilities to avoid duplication of effort and mentioned the potential liability issues that could arise if one party fails to fulfil its obligations. He prompted the participants to consider the implications of these factors within their respective ecosystems and whether they have discussed strategies to address these concerns.

Ashley Heineman, GoDaddy, acknowledged the complexity of compliance responsibilities and suggested that they may fall primarily on registrars, while **Michele Neylon, Blacknight**, highlighted the expected differences in the handling of regulations between the gTLD and ccTLD spaces. Michele also expressed concerns about potential data security issues and the varying levels of ISO certification among different registrars and registries. **Beth Bacon, PIR**, emphasised the importance of building trust and maintaining effective contractual relationships to ensure compliance, with particular reference to the forthcoming implementation of the Registry Data Policy. **Neal McPherson, IONOS**, described the power dynamics and potential imbalances in the business relationships between registries, registrars and resellers, emphasising the strategic considerations that come into play.

Samantha Demetriou, Verisign, raised concerns about the challenges that companies may face if they are tasked with enforcing compliance through their contractual arrangements. She emphasised the importance of assessing the adequacy of existing policies in the gTLD space and suggested that ICANN's policy framework could act as a backstop for compliance. **Volker Greimann, Team Internet**, supported this view, stating that ICANN's role should not be to duplicate what is already required by law and emphasising the need for ICANN to establish its own rules that are consistent with legal requirements without creating duplicative obligations or enforcement mechanisms.

Hadia El Miniawi questioned the benefit of having a multi-stakeholder group developing rules or policies that do not align with widely acknowledged laws and regulations. She wondered where this leaves the output of such a group.

In response, **Volker Greimann, Team Internet**, explained that international communities are creating minimum standards that individual countries or groups of countries can build upon as needed. Different countries may have specific requirements that go beyond these standards, but the goal is to strike a balance between global standards and local regulations. He highlighted China as an example with strict verification requirements and emphasised the importance of maintaining a balance without following a single, extreme model.

Neal McPherson, IONOS, considered whether validation can work effectively across various registries, including generic top-level domains (gTLDs) and country code top-level domains (ccTLDs). He discusses the incentives for registrars to implement scalable verification processes, ensuring cross-TLD validation. Collaboration between registries and ccTLDs in areas such as abuse prevention and technical policy is seen as an opportunity to enhance the effectiveness of validation across the domain registration ecosystem.

6.2 Creating standardised domain name verification processes

Creating standardised domain name verification processes across the industry to ensure a more streamlined and customer-friendly experience.

Pawel Kowalik, DENIC, suggested that registrars can act as intermediaries between registries and domain owners, helping to streamline the verification process if policies are aligned. This can create a relationship of trust between registrars and registries.

Chris Disspain, Identity Digital, expressed concern that different countries may have different verification tests and, without agreed standards, verification across different registries could be a challenge. He raised the question of whether there should be a standardised level of verification.

Samantha Demetriou, Verisign, raised concerns about the potential consequences of implementing standardised verification processes for both generic top-level domains (gTLDs) and country code top-level domains (ccTLDs). She fears that this could lead to the commoditisation of domain names, potentially reducing their distinctiveness. She also questioned the impact of such standardisation on competition.

Volker Greimann, Team Internet, proposed the idea of mutual recognition and acceptance of verification between registries and registrars. If a customer's domain ownership has already been verified through a verification scheme recognised by one registry, other registries could waive their verification process. This approach aims to make the process more customer-friendly and efficient.

Werner Staub, COREhub, pointed out that the market has developed solutions for verifying legal entities, such as the Legal Entity Identifier (LEI), which has been available for ten years. The LEI is a unique identifier that ensures the legal status of an entity, and many large companies with domain names already have it. However, there are no plans within ICANN to incorporate the LEI or similar identifiers into the data model. In addition, he mentioned the need to associate this identifier with domain names and to update the existing contact record model to include information about the level of verification performed on the association between a domain name and the verified identity. This suggests a potential way to improve the verification and validation process for domain holders.

6.3 What to do when validation fails?

Michele Neylon, Blacknight, raised a critical point about the challenges of implementing new policies for existing domain registrations. He stressed the complexity of managing long-standing domain registrations for large entities such as Fortune 500 companies or governments, particularly when faced with requirements that may require the suspension or deletion of such domains. **Beth Bacon, PIR**, added that the existing verification processes have been in place since at least 2013 and questioned how any changes to the verification requirements would affect these established registrations. Both Michele and Beth underlined the importance of considering the practical implications of enforcing new policies on existing domain registrations.

Ashley Heineman, GoDaddy, reinforced the perspective of many registrars who believe they are already compliant with existing requirements. She pointed to the tools and processes currently in place to address verification issues with customers and emphasised the need to carefully consider the implications of any new requirements.

6.4 How will registries and registrars handle disclosure?

Polina Malaja, CENTR, highlighted the intricacies of the disclosure clause and the 72-hour deadline for response, emphasising that NIS2 is not the only relevant legislation in the context of disclosure and that it doesn't in itself provide a legal basis for such actions. She underscored the importance of additional legislation, including the Electronic Evidence Regulation, which reflects the need to identify domain name holders and is primarily associated with criminal proceedings. Polina clarified that the response requirement in NIS2 doesn't explicitly address how disclosure should be made within the specified timeframe. She also touched on the importance of verifying the legitimacy of foreign law enforcement or other access seekers to ensure compliance with cross-border access rules.

Stressing the importance of risk-based decision-making, **Johannes Loxen, SerNet**, explained how his company assesses the potential consequences and associated risks of non-compliance. Taking into account the potential consequences, he emphasised the need to negotiate with lawyers when assessing whether to comply with certain legal requirements.

In response, **Peter Vergote, DNS Belgium**, stressed the importance of conducting a comprehensive risk assessment when evaluating access requests. The focus, he said, should not be solely on the legitimacy of the access seeker but rather on the risks associated with disclosing certain data. A thorough risk assessment process is necessary to ensure that registrars and registries do not inadvertently expose themselves to penalties or liabilities due to fraudulent access requests.

Thomas Rickert acknowledged the complexity of the issue and highlighted the existing pathways for disclosure based on legal requirements or legitimate interests. Each case needs to be assessed on its own merits to determine the appropriate approach, and careful judgement must be exercised when assessing requests to disclose data.

6.5 How does the timeline for NIS2 work with the necessary organisational and technical changes that might need to be made?

Beth Bacon, PIR, stressed the importance of the Registry Data Policy in facilitating the implementation of NIS2 compliance across different registry models. She highlighted the need for registries to move beyond basic compliance to a high standard of super-compliance with NIS2. This underlines the importance of the policy in guiding the necessary changes to ensure robust compliance.

Approaching the topic from a product management perspective, **Neal McPherson, IONOS**, focused on the customer experience in the domain registration process. He identified the competitive advantage of providing a seamless and supportive registration process, including verification, to guide customers effectively. The importance of building a system that can efficiently handle different verification models, lifecycles and communications to create a consistent and user-friendly experience for customers was also touched upon. Neal outlined a timeline for implementation, with the goal of having a comprehensive system in place by October 2024 to facilitate efficient domain registrations.

Volker Greimann, Team Internet, shared the challenging experience of implementing the eligibility checking requirements for .au domains, describing it as a "nightmare" to implement. He worried about the possibility of having to go through a similar process for the entire EU, highlighting the practical impossibility of such an undertaking.

Beth Bacon, PIR, focused on the importance of flexibility in the verification processes put in place by Member States. Overly granular and rigid verification processes may not be ideal, and she advocates a flexible approach that can accommodate different implementations. Beth raised the need for adaptable solutions as the regulatory landscape evolves, emphasising that GDPR and NIS 2 may not be the last regulations the domain industry will face.

7. A wish list for regulators

Thomas asked the speakers what they would like to see from regulators. **Beth Bacon, PIR**, expressed her wish for regulators to maintain flexibility and not ask for excessive detail. She emphasised the effectiveness of the multi-stakeholder model in addressing industry challenges. **Polina Malaja, CENTR**, also advocated for flexibility and technical feasibility, and she wanted regulators to be mindful of frictions that hinder verification processes and to remove them. **Ashley Heineman, GoDaddy**, wished for early engagement and dialogue between registrars, registries, and regulators to ensure a better understanding of operational constraints. **Volker Greimann**'s wish for regulators was "don't: less is more."

8. Maintaining an open dialogue

In his closing remarks, **Thomas Rickert** spoke of the importance of maintaining a strong connection and open dialogue between industry stakeholders and legislators. This communication is crucial to achieve a balance between regulation and flexibility, which in turn helps to build robust implementation models. The focus should be on legislation that sets minimum requirements while allowing companies to innovate and adapt within that framework.

He invited the NIS2 Cooperation Group to continue this dialogue between industry stakeholders and regulators committed to finding practical solutions that minimise friction and fragmentation in the market. The outstanding issues need to be addressed while there is still time to resolve them and work out how to implement the NIS Directive with the least friction and fragmentation in the market.

eco's Thomas Rickert (thomas.rickert@eco.de) and Lars Steffen (lars.steffen@eco.de) will gladly discuss how you can join the conversation.

NIS2

WORKSHOP REPORT

We thank the sponsors for their support of eco's ICANN78 Accompanying Programme:

CentralNic Registry
geoTLD.group promoting local digital identities
GoDaddy
Google
InterNetX
IONOS
iPHH
nameshield Online Assets Security
.org
RICKERT.LAW WIRTSCHAFT | DIGITAL | RECHT
team internet. group plc
VERISIGN

MOIN

*Moin Universal greeting in Hamburg that is used at all times of the day.

eco – Association of the Internet Industry
Lichtstr. 43h, D-50825 Cologne, Germany
phone: +49(0)221/700048-0
fax: +49 (0)221 / 700048-111
info@eco.de, https://international.eco.de
@eco_de, @ecoverband

eco
ASSOCIATION OF THE INTERNET INDUSTRY