EU Regulatory developments

What's in it for the DNS?

Polina Malaja
polina@centr.org

TLDCON 2021

16 September 2021

Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148 ('NIS2')

- 16 December 2020: Text in full available here
- ***Ex-ante*** **and** ***ex-post*** **supervisory regime** for "essential entities" (incl. TLDs) (Article 29/30).
- Administrative fines + additional penalties to essential and important entities (Article 31/33).
- The **management bodies of essential and important entities are accountable** for the non-compliance (Article 17).
- **'Data accuracy' obligation** on registries **and** registrars, including an obligation to provide personal data to 'legitimate access seekers' (Article 23)

Picture: European Commission

NIS2: What's in it for ccTLDs?

- Directive to apply **to all providers of DNS services along the DNS resolution chain**, including operators of root name servers, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers.
- **Maintaining accurate and complete databases of domain names and registration data** (so called 'WHOIS data') and **providing lawful access** to such data **is essential to ensure the security, stability and resilience of the DNS.**
- Potential 'legitimate access seekers': **public authorities, law enforcement authorities, CERTs, CSIRTs**, and as regards the data of their clients to **providers of electronic communications networks and services and providers of cybersecurity technologies.**
- **Jurisdiction:** main establishment in the EU; Non-EU TLDs: designated representative.

CENTR Comment on NIS2

Article 23

- **Clear purpose limitation** under the GDPR: “accurate data, having regard to the purposes for which it is processed”;
- Relevant information to identify and contact domain name holders **that is strictly necessary and proportionate** under the corresponding legal basis for such processing;
- Vague notion of **“complete” should be omitted;**
- Legitimate access seekers should be **limited to competent national authorities**, provided that access to registration data is granted under the corresponding legal basis that satisfies the conditions of the Union data protection framework.

The proposal for the Digital Services Act ('DSA')

- Legislative proposal: **15 December 2020** (full text)
- Targets all **"digital services",** incl. the ones not considered by the legislators in 1998-1999 → offering "network infrastructure"
- Revision of **intermediary** liability framework ('mere conduit', 'caching', 'hosting')
- **Jurisdiction:** main establishment; non-EU: legal representative.

Important Bits for ccTLDs

- ccTLDs considered **intermediaries**
- ccTLDs can be **exempt from liability case-by-case**, to the extent they can be considered 'mere counduit', 'caching', 'hosting'
- Concerns only **illegal content**
- **Voluntary own-initiative measures** to detect, identify and remove, or disable access to illegal content
- **No general obligation to monitor** for the illegal information
- **ccTLDs can receive judicial (or administrative) injunctions** requiring the termination or prevention of any infringement, including the removal of illegal content **National judicial or administrative authorities may order ccTLDs to act** against certain specific items of illegal content or to provide information

New obligations

	Intermediary services *(cumulative obligations)*	Hosting services *(cumulative obligations)*	Online platforms *(cumulative obligations)*	Very large platforms *(cumulative obligations)*
Transparency reporting	•	•	•	•
Requirements on terms of service due account of fundamental rights	•	•	•	•
Cooperation with national authorities following orders	•	•	•	•
Points of contact and, where necessary, legal representative	•	•	•	•
Notice and action and obligation to provide information to users		•	•	•
Complaint and redress mechanism and out of court dispute settlement			•	•
Trusted flaggers			•	•
Measures against abusive notices and counter-notices			•	•
Vetting credentials of third party suppliers ("KYBC")			•	•
User-facing transparency of online advertising			•	•
Reporting criminal offences			•	•
Risk management obligations and compliance officer				•
External risk auditing and public accountability				•
Transparency of recommender systems and user choice for access to information				•
Data sharing with authorities and researchers				•
Codes of conduct				•
Crisis response cooperation				•

CENTR recommendations

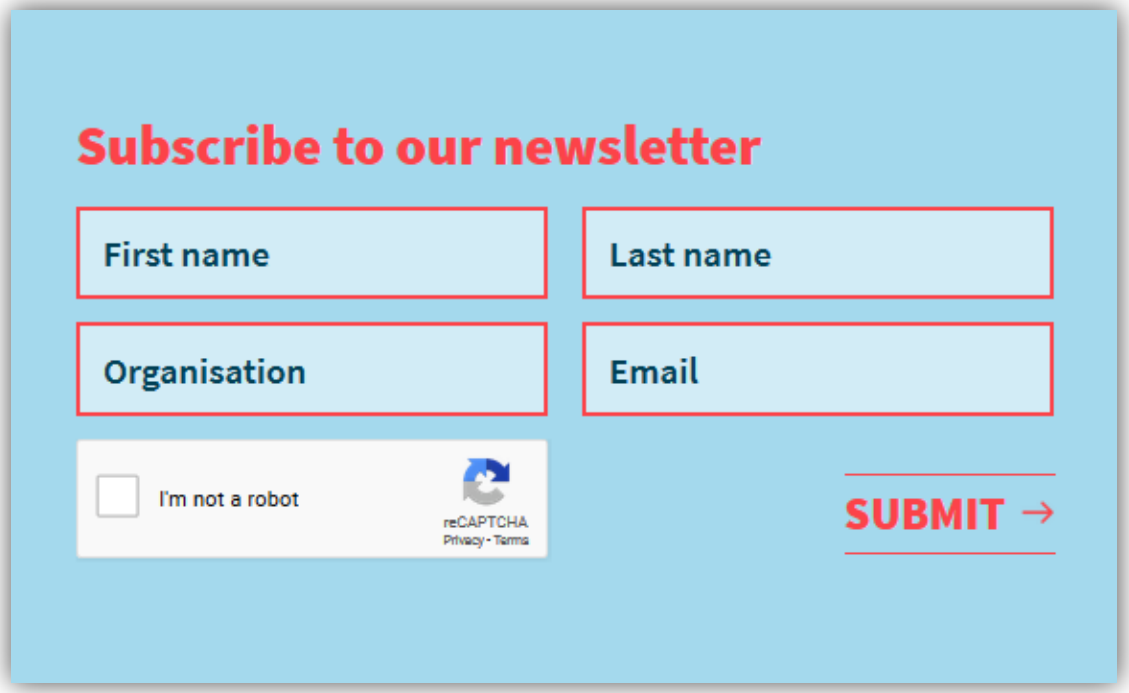
Summary of CENTR's key recommendations:

1. CENTR calls for an explicit liability exemption for the technical auxiliary function performed by DNS service providers, in the context of the provision of neutral DNS-related services for the functioning of other intermediary services.
2. CENTR calls for a clarification in the definition of illegal content. The current definition includes the vague wording 'by its reference to'. This inclusion could affect lawful reporting activities and even hamper the provision of technical auxiliary functions and, as such, could have a crippling effect on the functioning of the internet.
3. CENTR calls for an alignment of the powers given to Digital Services Coordinators with the criminal procedural law in the respective Member States, and an obligation for Digital Services Coordinators to demonstrate due diligence before resorting to exceptional powers under the Proposal.

CENTR comment on the DSA proposal (March 2021)

Stay informed!

Subscribe to all CENTR newsletters: visit centr.org



Thank you

polina@centr.org