PAC
#28

IE Domain Registry CLG
trading as .IE

Policy Advisory Committee – PAC #28

Minutes from the 15 July 2021 Meeting

We are
Ireland online

Table of Contents

Minutes of the PAC #28 Meeting held on 15 July 2021

Meeting Location: Virtual meeting.
Meeting Time: Called to order at 11:00am by the PAC Chair.
Members and representatives present:

Chair
CyberSafeKids
Department of Communications, Climate Action & Environment (DCCAE)
HEAnet
.ie Accredited Registrar (Blacknight)
.ie Accredited Registrar (Register Group)
.ie Accredited Registrar (MarkMonitor)
Irish Computer Society (ICS)
Irish Reporting & Information Security Service (IRISS)
Small Firms Association
IE Domain Registry CLG t/a .IE

1. Memberships Matters

Apologies – Members not present:

- Association of Patent and Trade Mark Attorneys (APTMA) – pre-arranged
- Enterprise Ireland – pre-arranged
- Law Society of Ireland – pre-arranged
- Internet Service Providers Association Ireland (ISPAI) – pre-arranged

2. Minutes from the 15 April 2021 PAC #27 meeting

The Chair confirmed that the Minutes from the PAC #27 meeting were published online (available here http://www.iedr.ie/policy-development-process/). It was noted that no requests for edits were made and accordingly, the minutes will be digitally signed by the Chair.

3. Matters arising

Matters arising included the PAC terms of reference, the EU's Digital Services Act, formal conclusion of the policy change request on reserved/blocked names and handling criminal abuse/illegality online.

- .IE confirmed that the PAC Terms of Reference (ToR) had been updated to reflect the new branding name of .IE, the new memberships and the previous edits, which included extending a 'Term' to four years. The updated ToR is published on the .IE corporate website here.

- Updates on the progression of the Digital Services Act will be dealt with by the external speaker, under item 5 on the agenda.

- The policy conclusion template on reserved/blocked names, is item 6 on the agenda. Following confirmation that all action items have been completed, it was agreed that the

Chair will digitally sign the Policy Conclusion template, on behalf of the PAC. The Chair thanked all members for their engagement on this topic.

- Regarding the matter of handling criminal abuse involving .ie domains:-

The registry provided a brief recap on the discussions and deliberations to date on the issue, including the presentation at PAC #23 from representatives of the GNCCB and GNECB on its reactive policing efforts to date, and the preference to shift to proactive, preventative policing to protect legitimate interest users from becoming victims of serious, life-altering crime.

The registry summarised the PAC's prior broad consensus in relation to a potential Cooperative Arrangement with law enforcement, provided it included; a structured process with appropriate safeguards that meet the needs of all stakeholders; that operated in a manner which is mutually beneficial to channel partners, and; only to be used where hosts had failed to address notified issues.

The registry confirmed that the draft Protocol document had been circulated to the wider Registrar channel. The feedback received was summarised on two slides (Appendix 1 – slidedeck) and additional details were provided by .IE staff.

In the ensuing discussion the following points were made:-

- Law enforcement generally does not understand what registrars can provide, and doesn't appreciate that registrars simply don't have some of the information requested.
- Based on her experience in the UK, a member said that National Units in the UK were trained and had developed experience over time, so they had a better understanding, and she gave the example of the child exploitation unit. She suggested that perhaps the solution might be to have multiple SPOCs, "single points of contact" per agency.
- In relation to the point about not informing the Registrant prior to suspension, a member suggested that .IE might look at the experience of the Canadian registry, whose protocol handled suspension requests for domains held by organised crime for instance.
- A member queried whether the proposed Protocol with GNCCB would be legally binding on registrars. There was a supplementary question on whether it might include an opt out clause, applied on a case-by-case basis by the registrar.
- Wrapping up the discussion, the Chair asked about the next steps and the endgame for the PAC.

In response .IE confirmed that it was seeking strong consensus from the registrar channel to adopt the protocol, however, there would be no obligation. Where a registrar had a pre-existing corporate policy or legal advice, .IE agreed that the protocol should provide for circumstances whereby registrars could opt out on a case-by-case basis.

Suggested next steps were to continue the engagement with the GNCCB in order to reach consensus on the protocol. Two Registrars representatives confirmed their availability to join in those discussions with the GNCCB at the appropriate time.

4. Handling of online abuse which uses the .ie namespace

4.1 Technical abuse - Netcraft experience since 1st March soft launch

The registry confirmed that the Netcraft service launched on 1st March, following the negotiation of contractual terms and conditions with Netcraft, and confirmation that costs for the initial period would be paid by .IE.

The current stats on the cases handled by the Netcraft service was illustrated on the slides. The Chair asked that these be taken as-read, in the interests on time management. Members were asked to revert with any queries to .IE. This was agreed by participants.

5. NIS 2 – Role for the PAC ?

The context was set for the discussion by asking if there was a role for the PAC in relation to preparing the local Internet community in Ireland for the introduction of a new Directive on the Security of Network & Information Systems (NIS 2).

A guest speaker from the CENTR organisation, Polina Malaja, Policy Advisor, provided a comprehensive update of the status of the draft Directive. (Presentation slide deck - Appendix 2).

The speaker highlighted the relevance of the Directive, clarifying that TLD registries and Registrars were firmly in scope, even though micro and small entities were generally excluded. For the newly defined “important entities”, the limited supervisory regime will be ex-post (following an incident). However for “essential entities” there is a proposed ex-ante and ex-post supervisory regime.

The speaker highlighted the “data accuracy” obligations on registries and registrars, including an obligation to provide registrant’s personal data to “legitimate access seekers” set out in the contentious Article 23. The potential conflict with the GDPR provisions on minimising processing of personal data was summarised.

The speaker provided an extremely informative behind the scenes view on the drafting and negotiation processes within the EU bodies:-

- Three committees within the European Parliament are examining the subject:-
  - Industry, Research and Energy (*ITRE*).
  - Internal Market and Consumer Protection (*IMCO*).
  - Civil Liberties, Justice and Home Affairs (*LIBE*).
- The co-legislators, (the Parliament and the Council) will attempt to finalise their respective positions on NIS2 before entering into trilogue negotiations with the Commission during 2022.

The best estimate of the indicative Timetable for implementation in Ireland is dependent on the above processes in Europe. The speaker said that trilogues are expected to start by the end of 2021. The best case scenario for a conclusion of the trilogues, and adopting the Directive, is by the end of 2022. Member States will then have 18 months to implement changes in their national legal frameworks.

Finally, the speaker provided an update on the progress of the Digital Services Act (DSA), which involves the revision of the e-commerce Directive, and targets all “digital services”. Referring to the CENTR comment document on the DSA proposal, issued in March 2021, the speaker

highlighted its call for an explicit “liability exemption” for DNS service providers on the basis that they are ‘mere conduits’, and also the call for clarification in the definition of “illegal content”.

Following a brief Q&A, the Chair thanked our CENTR guest speaker on behalf of the committee members.

There followed a presentation “NIS2 roadmap for Ireland” by the PAC representative from the Department of Communications (DCCAE) Mr Fergal Corcoran, speaking on behalf of the NCSC. He invited active engagement from all parties with the NCSC & the Department, whether individually or separately, on the basis that it was important that all views and opinions were passed on.

During the subsequent discussion, a Registrar representative complemented the CENTR document submitted to the EU and also highlighted the imminent danger that trademark protection lawyers were seeking to overturn data protection provisions within the GDPR.

It was agreed that all parties will continue to monitor NIS2 developments, to share feedback on the outcome of various consultations and to engage with their motherships in order to formulate opinions on the way forward.

The Chair thanked members for their engagement, and summarised that there was an emerging consensus that the PAC could play an important role and should get involved. This will be dealt with at the next PAC meeting.

6. Any Other Business

6.1. Update from PAC members on industry sector developments/legislative changes

This item was carried forward, in the interests of time management.

7. Next Meeting

The provisional date for the next PAC meeting has been set for Thursday 11th November 2021.

Appendices

1. PAC #28 slidedeck from 15 July 2021
2. CENTR presentation slides - Polina Malaja, Policy Advisor, CENTR

We are Ireland online

Policy Advisory Committee

15 July 2021

Meeting - PAC#28

Policy Advisory Committee - Agenda

1. Membership Matters
2. Minutes from the PAC#27 meeting
3. Matters arising
4. Handling of online abuse which uses the .ie namespace
5. NIS 2 – Role for the PAC ?
6. Policy Conclusion template
7. Any Other Business
8. Next Meeting

1. Membership Matters

- Please keep **microphones muted** throughout the call
- Please **“raise a hand”** to ask a question or **add comments** in the chat box
- Request to allow the meeting be **recorded** to assist with minute drafting
  - Recording will deleted once the Minutes are approved by PAC

2. Minutes of the PAC #27 Meeting

- Meeting minutes are circulated to the membership within one week of each meeting
- Comments/feedback accepted over a two week period
- If clarifications/edits are requested, and consensus exists, these are reflected in the Minutes
- Meeting minutes, and supporting slides, are published on weare.ie after the comment period has ended
- Published online at https://www.weare.ie/policy-development-process/

3. Matters arising

- Policy conclusion template:- reserved/blocked names
- PAC Terms of Reference
- Digital Services Act
- illegality online - engagement with GNCCB

We are Ireland online

3. Matters arising

Handling of illegality and criminality in the .ie namespace

- Common Ground

- Remaining matters
  - Issue requests from a single point of contact
  - Name / Rank of requesting officer
  - Document – wet signature
  - Sequence of engagement
  - Informing the registrant
  - Basis for refusal

3. Matters arising

Handling of illegality and criminality in the .ie namespace

- Have an agreed, defined, transparent process for handling abuse associated with .ie domains
  - One request - for transparency biannual reports on issues should be made public
  - One comment – the processes and policies should not be overly prescriptive

- The Registrar should not be the first line of approach for a domain suspension or deletion request from law enforcement
  - It should be the registry
  - It should be a multipronged approach - registrant first, then hoster, then Registrar, then Registry

- Request signed by a Garda at the rank of Inspector, or above, at a minimum
  - One comment - a court order is preferable

We are Ireland online

3. Matters arising

Handling of illegality and criminality in the .ie namespace

- Registrar - respond to a request from the ***local*** Garda Inspector, or single point of contact (GNCCB)
  - Some refer Gardaí to the Registry
  - Some deal with local Gardaí already
  - Some would prefer a court order to take action
  - One suggestion - requests should come from the GNCCB directly to the Registry

- Scenarios where you would not comply with a request from the GNCCB
  - Where clear evidence isn't supplied
  - Where there are inaccuracies or incomplete information
  - Will refer it to the Registry
  - A court order is preferable in some or all instances

4. Update on handling of online abuse in the .ie namespace

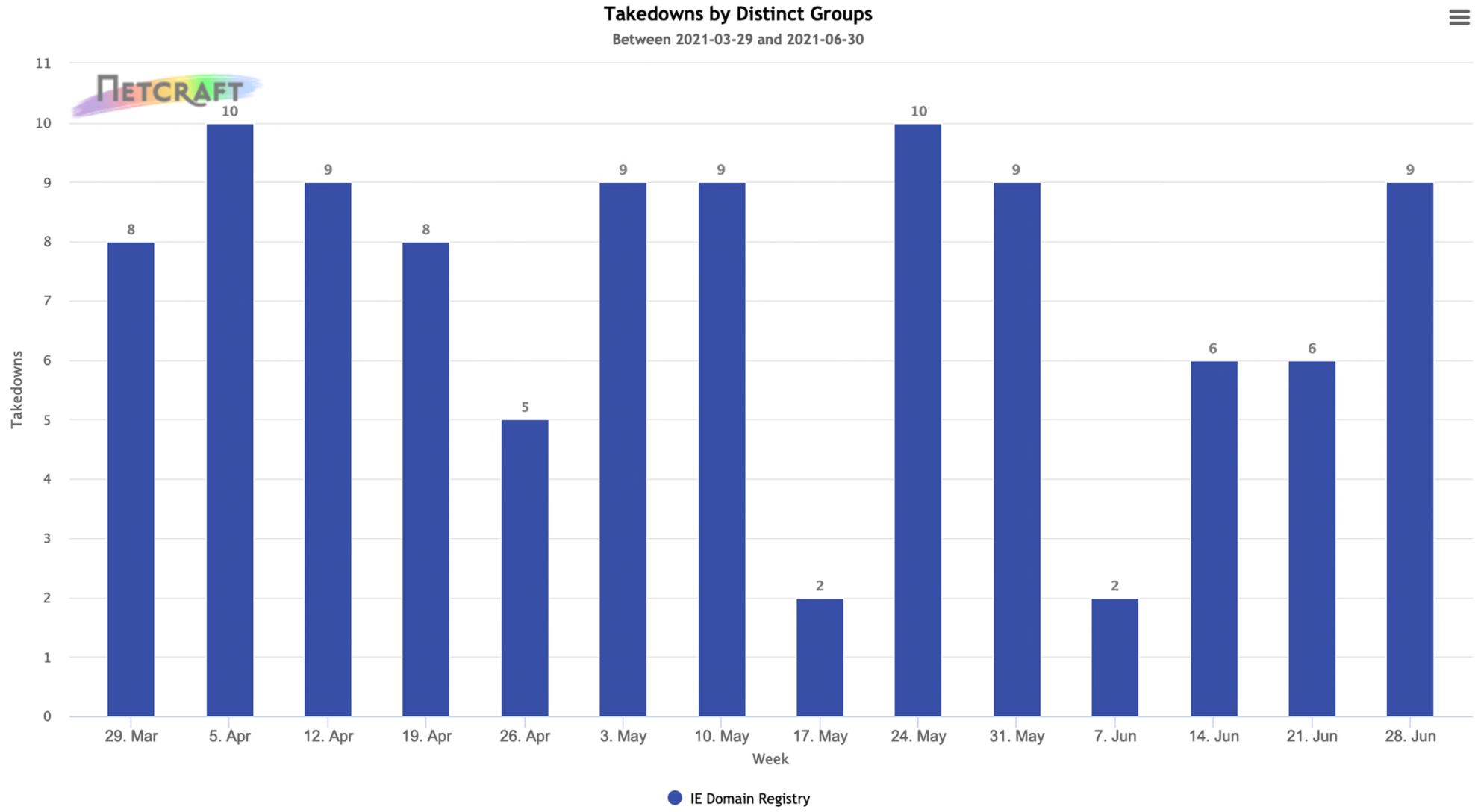
Technical abuse:- use of Phishing, Malware, botnets etc

Feedback on Netcraft service during Q2:-

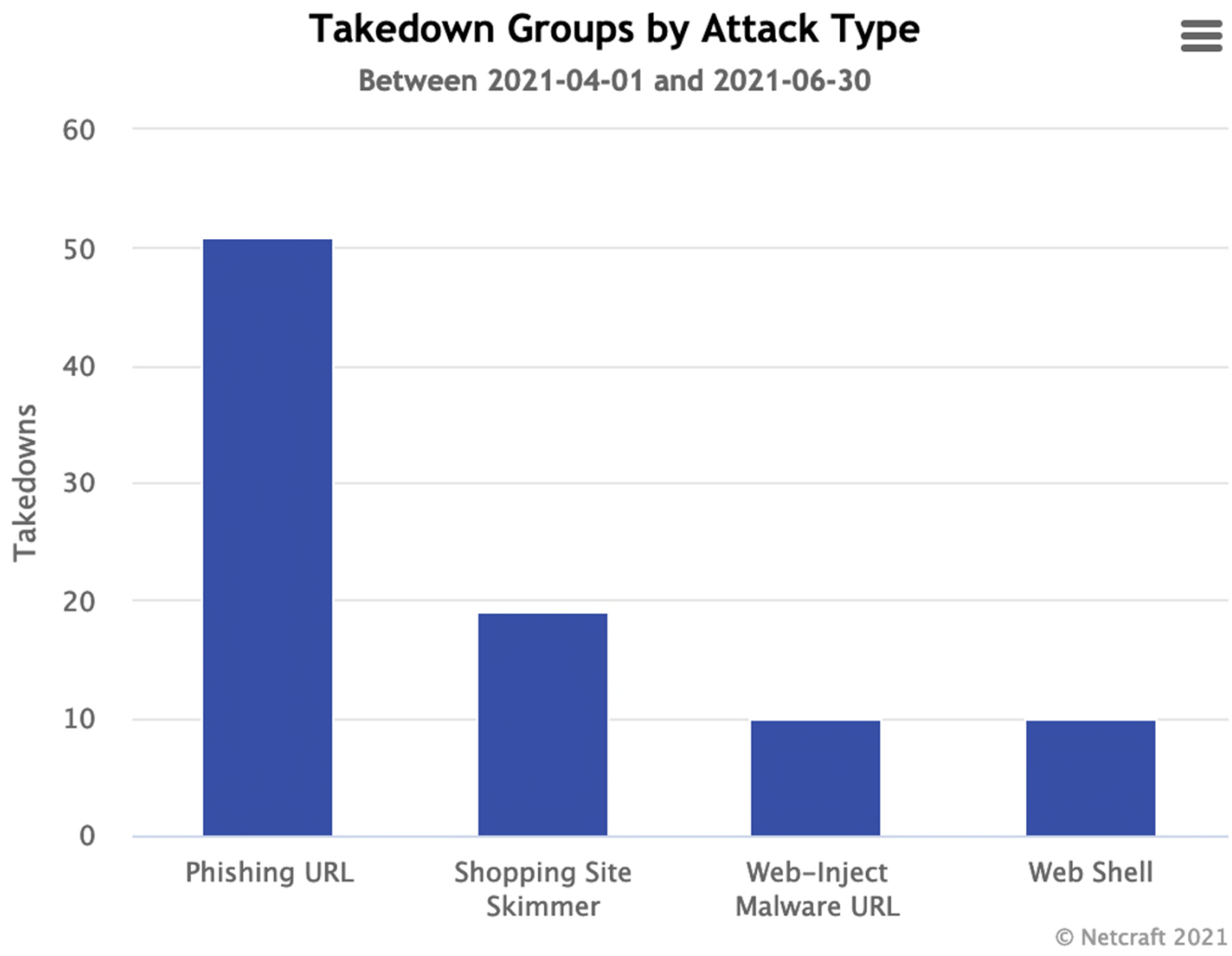
- 90 attacks
- 86 are down
- 4 are still active

Highest profile domain is http://www.irishlifeandpermanent.ie

4. Update on handling of online abuse in the .ie namespace



4. Update on handling of online abuse in the .ie namespace



5. NIS2 – Role for the PAC ?

- Guest Speakers
- Open discussion
- Role for the PAC ?

6. Policy Conclusion Template

- 6.1. Policy change - handling of reserved/blocked names

7. Any Other Business

Policy Change Request

***Request**:- In order to sell products on a ".ie" website the company needs to be Irish VAT Registered.*

Purpose & benefits:- These unscrupulous websites are set up to fool Irish people into thinking they are buying Irish but they are not buying Irish and the purchases are subject to additional import charges.

Grounds:-

There are several UK websites that have a ".ie" website. When an Irish consumer purchases from these the purchases are then subject to an import VAT charge.

This causes reputational damage to the ".ie" as I had assumed a ".ie" meant it was Irish but it doesn't and example of this type of website would be https://www.blindsdirect.ie/

8. Next Meeting

Proposed date:

16th September 2021

We are Ireland online

Policy Advisory Committee

15 July 2021

Meeting - PAC#28

EU Policy & Legislative Update

Polina Malaja
polina@centr.org
.IE Policy Advisory Committee Meeting
Virtually everywhere
15 July 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
- Exclusion of micro- and small entities from the scope (**except TLDs and DNS service providers** (!); Article 2(2))
- *Ex-post* supervisory regime for "important entities", ***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

Article 23: What's in it for ccTLDs?

- DNS is "a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend" (Recital 15).
- **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 (Recital 59, Article 23)
- Potential 'legitimate access seekers': **public authorities, including competent authorities** under Union or national law for the prevention, investigation or prosecution of criminal offences, **CERTs, CSIRTs**, and as regards the data of their clients to **providers of electronic communications networks and services and providers of cybersecurity technologies** (Recital 60).
- The access procedure may also include the use of an interface, portal or other technical tool to provide **an efficient system for requesting and accessing registration data**.[...] the Commission **may adopt guidelines** on such procedures without prejudice to the competences of the European Data Protection Board (Recital 61).

CENTR Comment on NIS2

Available here

- **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**, as designated by Member States under their national cybersecurity strategies, including national law enforcement authorities, provided that access to registration data is granted under the corresponding legal basis that satisfies the conditions of the Union data protection framework.

NIS2: developments in the European Parliament

- European Parliament's ITRE: Draft Report
  - → Obligation to “verify”, in addition to “accurate and complete”
  - → “relevant information”: registrants' name, physical, email address, telephone number
  - → reply in any event within 72 hours to all requests for access to non-public registration data
  - → legitimate access seekers: for example for cybersecurity reasons, detection and prevention of crime, protection of minors and intellectual property, fraud prevention and protection against hate speech

- European Parliament's IMCO: Draft Opinion (CA)
  - → Obligation to “verify” “accurate and complete” registration data “necessary for the provisions of their services”
  - → “relevant information”: registrants' name, physical, email address, telephone number
  - → inaccurate or incomplete data should be corrected or erased by the registrant without delay
  - → reply in any event within 72 hours to all lawful and duly justified requests for access

NIS2: developments in the European Parliament

- European Parliament's LIBE: Draft Opinion
  - → "relevant information": registrants' name, physical address, email address, telephone number
  - → publish domain name and the name of the legal person
  - → reply without undue delay to all lawful and duly notified requests for access
  - → "legitimate access seekers": competent authorities under this Directive or supervisory authorities under Regulation (EU) 2016/679

Timetable (indicative):

- → Vote on the main ITRE Report: preliminarily in October; Plenary TBC
- → Trilogues to start by the end of the year
- → Adoption depends on the trilogues: the best case scenario for co-legislators in 2022
- → DIRECTIVE: 18 months for Member States to implement changes in their national legal frameworks

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

- Legislative proposal: **15 December 2020** (full text)
- Revision of **e-Commerce Directive** (2000)
- Targets all **"digital services",** inlc. the ones not considered by the legislators in 1998-1999 → offering "network infrastructure"
- Revision of **intermediary** liability framework ('mere conduit', 'caching', 'hosting')
- Gatekeeper platforms; cloud service providers; app stores; "very large online platforms" etc.

Important Bits for ccTLDs

- ccTLDs considered **intermediaries** (Rec 27, 83)
- ccTLDs can be **exempt from liability case-by-case**, to the extent they can be considered ‘mere counduit’, ‘caching’, ‘hosting’ (Rec 27)
- Concerns only **illegal content** (Rec 12)
- **Voluntary own-initiative measures** to detect, identify and remove, or disable access to illegal content do not strip intermediaries from liability exemptions (Art 6)
- **No general obligation to monitor** for the illegal information (Art 7)
- **ccTLDs can receive judicial (or administrative) injunctions** requiring the termination or prevention of any infringement, including the removal of illegal content (Rec 24, Art 8)
- **National judicial or administrative authorities may order ccTLDs to act** against certain specific items of illegal content or to provide information (Rec 29, Art 8, 9)

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				•

Important Bits for ccTLDs

- ccTLDs considered **intermediaries** (Rec 27, 83)
- ccTLDs can be **exempt from liability case-by-case**, to the extent they can be considered ‘mere counduit’, ‘caching’, ‘hosting’ (Rec 27)
- Concerns only **illegal content** (Rec 12)
- **Voluntary own-initiative measures** to detect, identify and remove, or disable access to illegal content do not strip intermediaries from liability exemptions (Art 6)
- **No general obligation to monitor** for the illegal information (Art 7)
- **ccTLDs can receive judicial (or administrative) injunctions** requiring the termination or prevention of any infringement, including the removal of illegal content (Rec 24, Art 8)
- **National judicial or administrative authorities may order ccTLDs to act** against certain specific items of illegal content or to provide information (Rec 29, Art 8, 9)

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)

DSA: developments in the European Parliament and Council of the EU

- European Parliament's IMCO Draft Report

→ "Know-Your-Business-Customer" (KYCB) obligation on all intermediaries, including TLD registries and content delivery networks

→ due diligence checks to **verify** business user information *prior to the use of the service*

→ store all information in a secure manner so that it can be **accessed by public authorities and private parties with legitimate interest**

→ Obtain information such as name, address, phone number, email, a copy of identification document, bank account details, business registration number

→ in case business user fails to correct/complete that information to suspend the provision of its service to that user

- Council of the EU (compromise text by Portuguese presidency)

→ limits the KYCB to online marketplaces but references NIS2 in connection to traceability of domain name holders

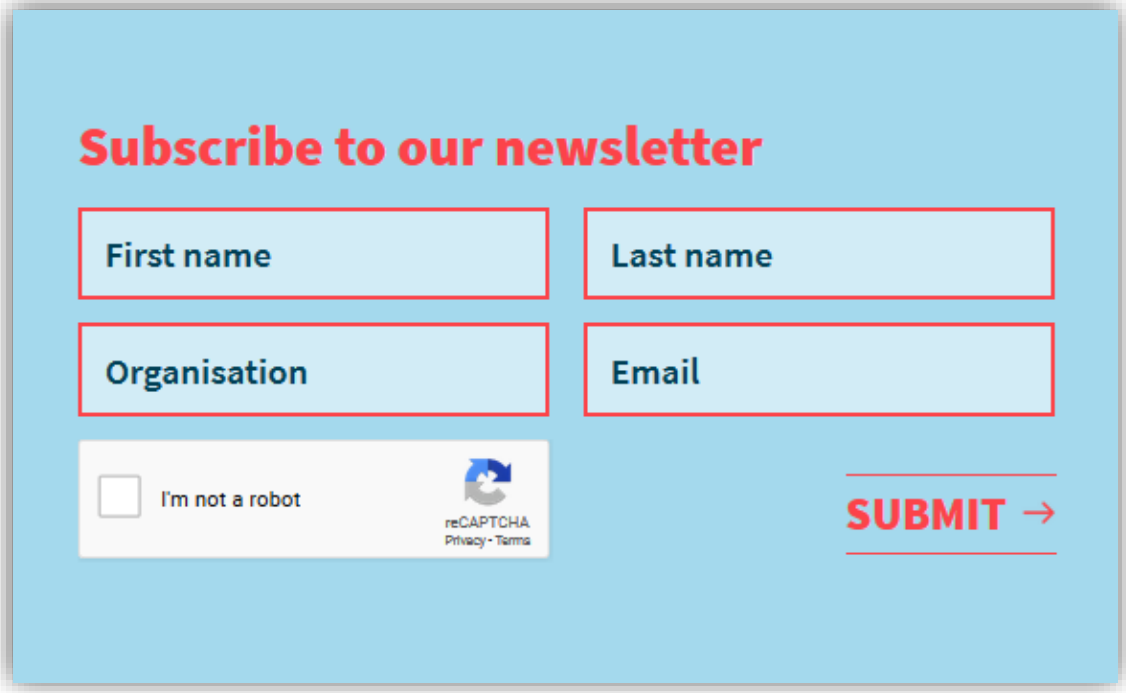
DSA: developments in the European Parliament and Council of the EU

Timetable (indicative):

- Vote on the main IMCO Report: preliminarily in November; plenary vote in December
- Trilogues to start in 2022
- Adoption depends on the trilogues: the best case scenario for co-legislators by the end of 2022
- REGULATION: directly applicable in Member States three months after its entry into force

Stay informed!

Subscribe to all **CENTR newsletters**: visit **centr.org**



Thank you

polina@centr.org