



We are
Ireland online

Policy Advisory Committee

14th September 2023

Meeting – PAC #36

Policy Advisory Committee

Agenda PAC #36

1. Membership Matters
2. Minutes from the PAC #35 meeting
3. Matters arising
 - *Proposal for Miscellaneous Amendments to the .ie Policy Suite*
4. Handling of online abuse which uses the .ie namespace
 - *4.1 illegality online (amending the RAP protocols)*
 - *4.2 tech abuse (Netcraft stats)*
5. NIS 2 update
6. AOB
7. 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 be deleted once the Minutes are approved by PAC

2. Minutes of the PAC #35 Meeting

- Meeting minutes are circulated to the membership promptly after 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](https://www.weare.ie) after the comment period has ended
- Published online at <https://www.weare.ie/policy-development-process/>

3. Matters arising

Misc. Amendments to the .ie Policy Suite

- Policy Proposal to make **non-substantive** amendments to the .ie Policy Suite:
 - Policies have not been updated since 2020. Not reflective of significant changes.
 - Proposal will remove out-of-date information (i.e., references to iedr.ie, or the IEDR Console)
 - Will be seeking an expedited process due to the non-substantive nature of the proposal

- Future proposals for re-structuring the .ie Policy Suite anticipated in the lead up to NIS2
 - Proposals will likely be non-substantive, and only deal with formatting and structure
 - NIS2 will bring significant policy changes – better to deal with structure and formatting first

3. Matters arising

- Domain Alert System (DIAS) to protect products with geographical origin and reputation:-
 - craft and industrial products (e.g Donegal Tweed)
 - wine, spirit drinks & agricultural products

- Disagreement between Parliament and Commission
 - New or existing processes & systems?
 - To be resolved in trilogue negotiations during 2023

- Why is the CIGI issue so important for Ireland?

*CIGIs - regulation on geographical indication protection
for craft and industrial products*

3. Matters arising

EU GI scheme for craft and industrial products

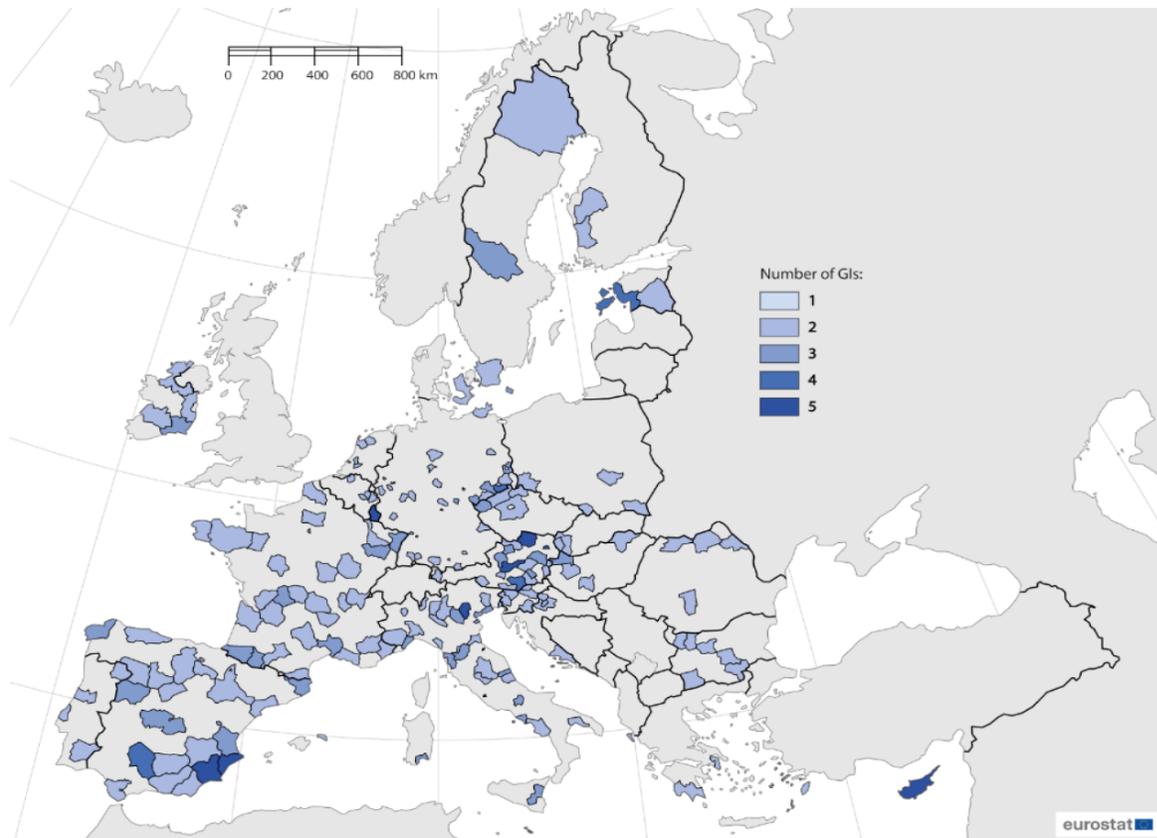


‘Indications which identify a good as originating in the territory of a Member, or a region or locality in that territory, where a given quality, reputation or other characteristic of the good is essentially attributable to its geographical origin’

² (WTO TRIPS Art.22, WIPO Geneva Act Art.2(1)(ii))

3. Matters arising

Economic context



Note: The picture maps 300 craft and industrial products identified in VVA *et al.* (2020) into nuts3 regions.

- 80% of CI GI products are made by **small and micro enterprises**



- **Located in less developed regions:** 75% of the regions with CI GI products have either GDP per capita or unemployment rate below the EU average

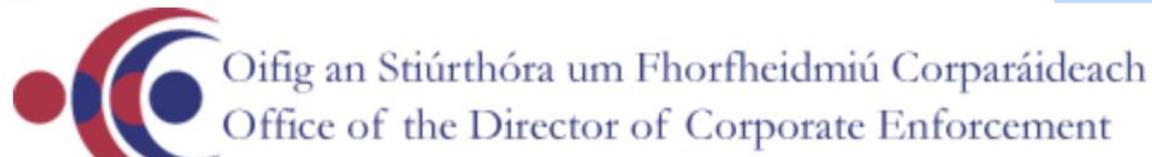


- CI GI products are located in the regions with significantly higher **vulnerability in the tourism sectors** when compared to regions without geographically rooted products

4.1 Handling of illegality and criminal abuse in the .ie namespace

Recap

We have established consumer protection protocols following due process with regulators and others to address online **illegality / criminality** which involve registry and registrars' coordination and cooperation.



~ Corporate Enforcement Authority

4.1 Handling of illegality and criminal abuse in the .ie namespace

Types of Requests from Regulators & National Authorities

Takedown

- This must be done at the Registrar Level. Regulators seeking the permanent deletion of a website should contact Registrars first for quickest resolution (Usually reserved for CSAM, trafficking, criminality or cyber security).

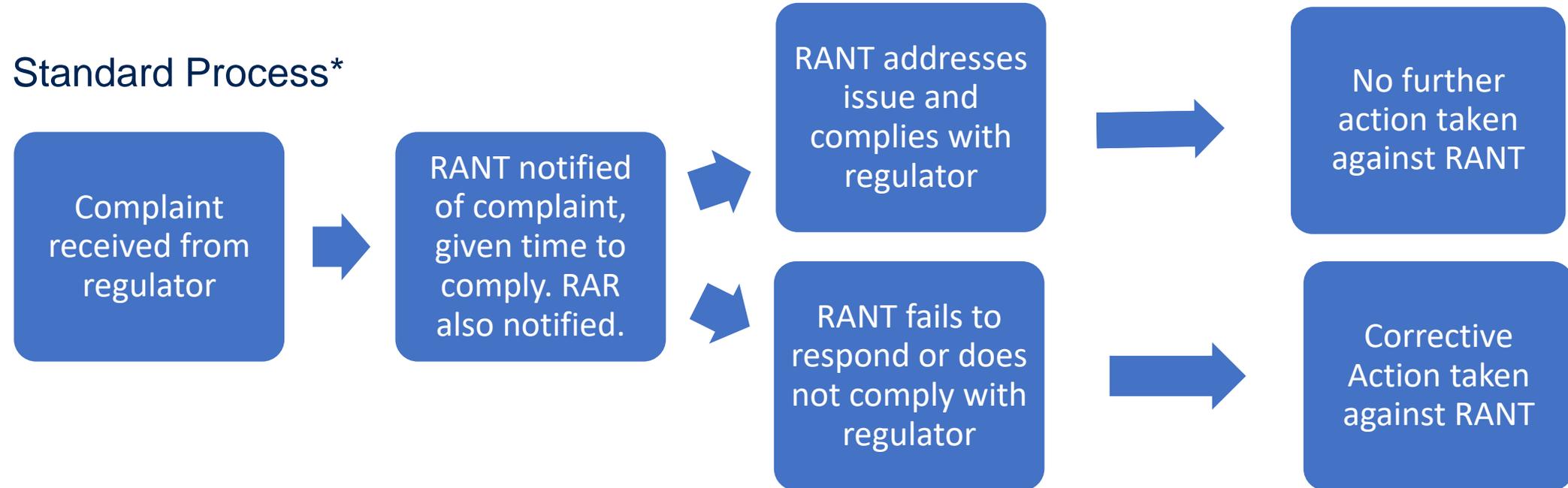
Suspension

- The most common request. Regulators may seek a domain name to be immediately suspended to prevent consumer access to the website. Access is still possible with a known IP address. Domain names may be suspended while a resolution is being reached, or a takedown arranged.

Resolution

- Unless otherwise requested, the standard process is to engage with the RANT and seek a resolution before any corrective actions are taken (generally relating to web content or fake web shops).

4.1 Handling of illegality and criminal abuse in the .ie namespace



*Due to the possible severity of their requests (CSAM, trafficking, etc.), the GNCCB process involves contacting the Registrar first for takedown

4.1 Handling of illegality and criminal abuse in the .ie namespace

Updates

- Creating a **common template** for regulators to submit complaints under the Regulatory Authority Protocol
 - Currently regulators submit complaints through different methods (CCPC has their own form, ad-hoc email requests have come from other regulators like HPRA, Royal Institute of Architects, etc.)
 - Only the GNCCB has a dedicated form to submit a complaint under the RAP
- Considering expanding the **GNCCB protocol** for other law enforcement agencies (Economic Crime Bureau, Criminal Assets Bureau, Drugs & Organised Crime Bureau, etc.).
- Separately, .IE is also creating a formalised template to process and review requests from regulators that request a **disclosure of registration data**, in accordance with .ie's Privacy Policy:
 - "We do not disclose your personal information to any third parties, other than:*
 - *with Irish national law enforcement agencies and Regulatory Authorities,"* etc...

4.2 Handling of technical abuse

Netcraft monitoring service

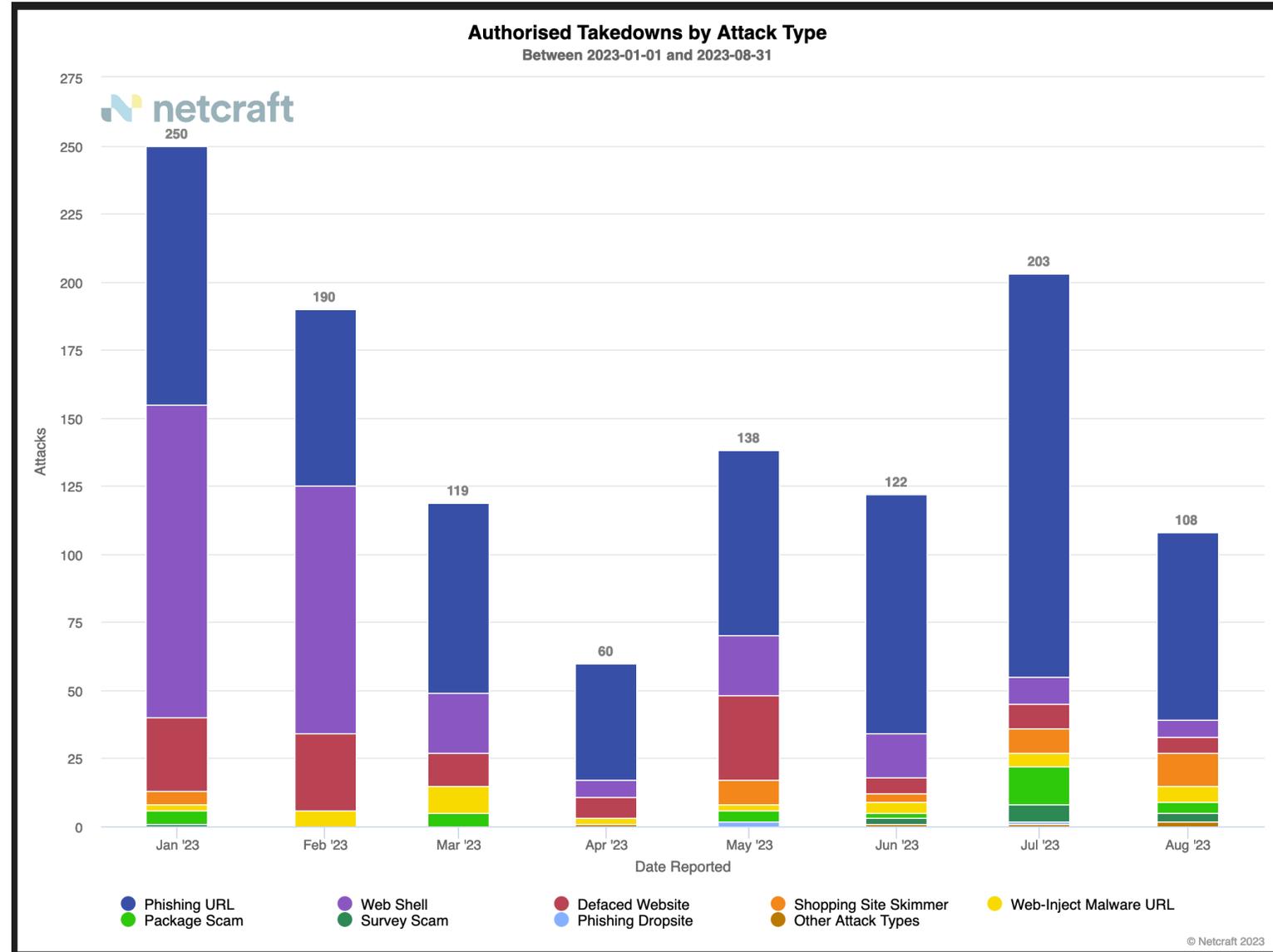
Recap

- Consensus from PAC members
- Service commenced March 2021
- Registrar's role
- Financed by .IE
- Benefits:
 - Proactively respond to technical abuse (e.g. malware, phishing or botnets)
 - Helps innocent victims (e.g. SMEs who might be unaware that they have experienced a cyber attack)
 - Notification allows them to take the required remediation action

4.2 Handling of technical abuse

Handling of online
Technical abuse:-
use of Phishing, Malware,
botnets etc...

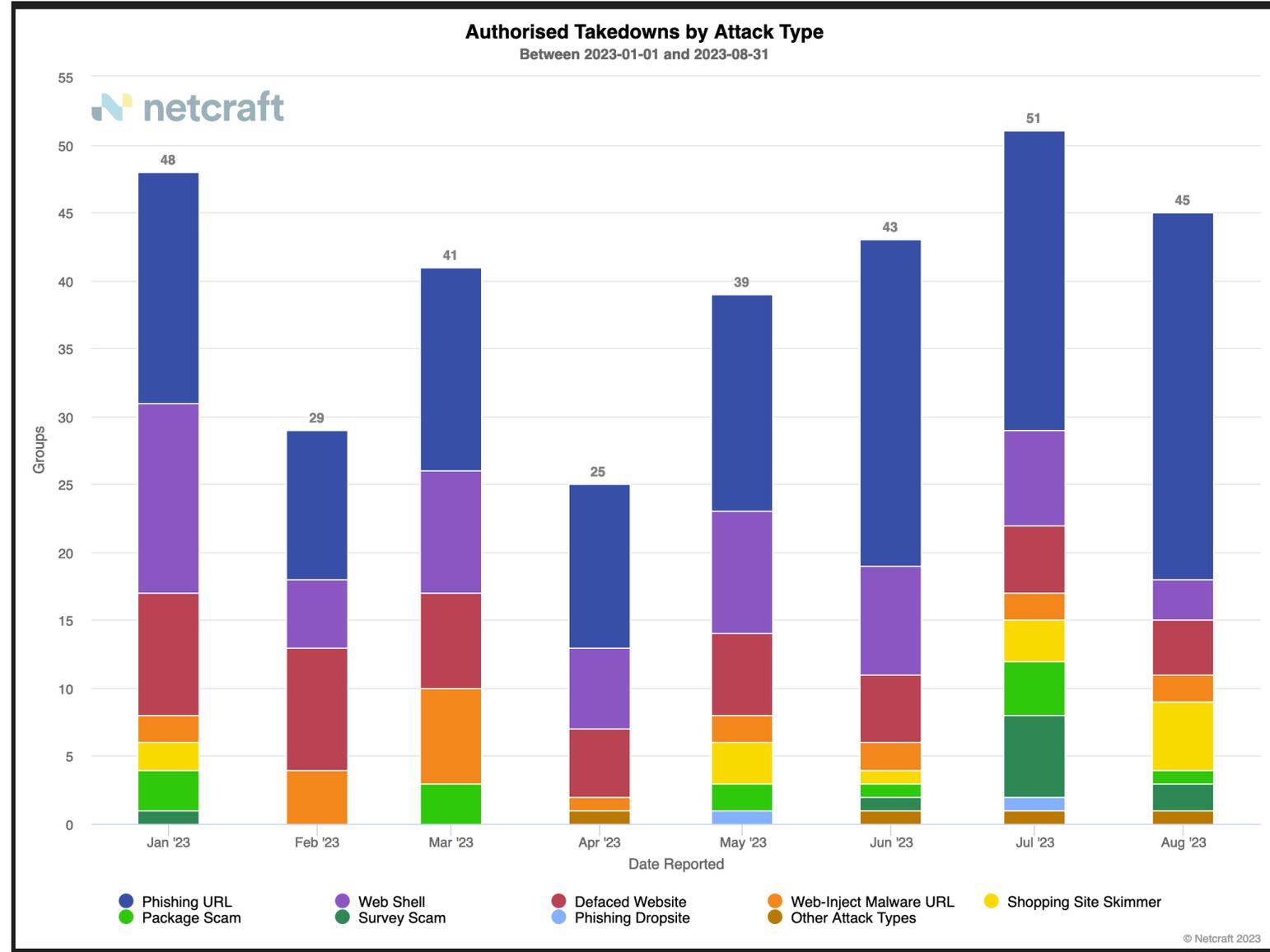
Netcraft service:-
1,190 attacks
1 Jan'23 to 31 Aug'23



4.2 Handling of technical abuse

Handling of online **Technical abuse**:-
use of Phishing,
Malware, botnets etc

Netcraft service:-
321 takedowns
1 Jan'23 to 31 Aug'23



5. NIS 2 – Directive on security of network & info systems

RECAP

➤ Concentrate effort into 3 Focus Areas:

- **Alignment** – Ensure that .IE policies and procedures comply with legislation.
- **Advocacy** – Frequently collaborate with policymakers and present the concerns of stakeholders.
- **Awareness** – Inform stakeholders of upcoming changes, and preparing them for policy changes.

➤ Key Deliverables Include:

- **Impact Report** – Report on potential impacts of NIS2 on the .ie namespace.
- **What-We-Heard Report** – Report summarizing stakeholder input, and partners' input.
- **Policy Options** – An evergreen document of proposed policy changes. Updated as legislation progresses.
- **White Papers/Open Letters/Blogs, etc...** – Products used for consultations, advocacy, and awareness building.

➤ Key trade offs that must be balanced:

- **Effectiveness** – Does the policy address the issue (is it compliant with NIS2?)
- **Efficiency** – Is the policy scalable and not unduly burdensome?
- **Equitability** – Does the policy unduly disadvantage, or advantage, any particular group?
- **Enforceability** – Is the policy reasonable to expect, and impose, compliance upon?

5. NIS 2 – Directive on security of network & info systems

5.1 NIS2 Mandate Tracker Actions taken since last PAC Meeting (14 May 2023)

<h3>Alignment</h3> <p>Ensure that .IE Policies and Processes are aligned with NIS2 requirements</p>	<h3>Advocacy</h3> <p>Frequently present the concerns and views of stakeholders to policymakers</p>	<h3>Awareness</h3> <p>Actively inform Registrars of impending changes from NIS2</p>
<div data-bbox="321 644 614 936" style="text-align: center;">  <p>3 Actions taken</p> </div>	<div data-bbox="1123 644 1416 936" style="text-align: center;">  <p>2 Actions taken</p> </div>	<div data-bbox="1926 644 2219 936" style="text-align: center;">  <p>1 Action taken</p> </div>
<ul style="list-style-type: none"> • Impact Analysis conducted and reviewed by WG (11 July 2023) • Discussions on Article 28 & Article 21 Policy Issues held by WG (10 Aug 2023) • Jurisdiction Scan of CENTR partners (ongoing) 	<ul style="list-style-type: none"> • Results from survey and insights from stakeholder engagement emailed to DECC officials (July 2023) • What We Heard Report being drafting based on early engagement (pending) 	<ul style="list-style-type: none"> • Developing engagement plan for informing larger RAR channel (webinars?)

5. NIS 2 – Directive on security of network & info systems

5.2 Key Emerging Issues - Updates from CENTR & fellow ccTLDs across EU

- Several ccTLDs have commented their governments are considering burdensome legislation beyond the minimum requirements of NIS2
- CENTR L&R Workshop upcoming (Sept 25/26) – More updates expected.
 - Almost all sessions related to NIS2 compliance.

5. NIS 2 – Directive on security of network & info systems

5.3 Updates from the NIS2 working group

(Meetings on 11 July & 10 August 2023)

- Met on **11 July 2023** to review an initial impact analysis from .IE. Identified high-risk issues were:
 - Issue 1 - Collection and Maintenance of Accurate & Complete Registration Data (KYC)
 - Issue 2 - Provision of Registration Data Access to Legitimate Access Seekers
 - Issue 3 - EU-Wide Cybersecurity Measures
- General consensus was these were appropriate areas to focus efforts on.
- Met on **10 August 2023** to discuss early policy considerations:
 - Who should be responsible for KYC? (RGY, RAR, Hybrid, Third Party?)
 - How can the Registry support Registrars in meeting Article 21 cybersecurity requirements?
- No consensus reached on responsibility for KYC.
- On Article 21, consensus reached that the RGY should aim to motivate & incentivise RARs (avoid penalising)

5. NIS 2 – Directive on security of network & info systems

5.4 Discussion – KYC Responsibility

- NIS2 will require (at minimum) the following domain registration info to be verified:
 - Domain name
 - Date of registration
 - Registrant name, email & phone
 - AdminC (if different than RANT) email & phone

- Where should responsibility for verifying this information fall?
 - Registry?
 - Registrar?
 - Mixture of both? A third party KYC provider?

6. AOB



6.1 EU regulatory environment

6.2 Ireland's Online Safety and Media Regulation (OSMR) Act 2022

6.3 Online safety commissioner

6.4 Registrar representative vacancy

6. AOB

EU Policy Update – Summer 2023

- The European Commission has published its strategy on **Web 4.0** and virtual worlds.
- Trilogues on the **agricultural geographical** indication proposal continue after the summer break.
- A Proposal on Financial Data Access implicates domains.
- The European Commission adopted an adequacy decision on the **EU-US Data Privacy Framework**.
- The **ENISA** mandate and EU cybersecurity certification framework are up for evaluation.
- The path toward trilogues on the **Cyber Resilience Act** is clarified.
- Spanish Presidency issued compromise text on the Proposal to combat child sexual abuse online (**CSAM**)
- For some very large actors, the **Digital Services Act** has started taking effect.

7. Next Meeting

Proposed date:

30th November 2023