

# Abuse prevention: Sharing indicators

Jordi Iparraguirre – Innovation manager - EURid

ICANN 74 – Den Haag – 2022.06.13

# What's all about

- Presented in the last CENTR Meeting – Prague 2022.05.31
- Shared at ccNSO TechDay to:
  - Inform other ccTLDs
  - Collect input if other ccTLDs are already doing something similar

dnsbelgium

.dk hostmaster

eu  
Powered by EURid

eu  
Powered by EURid



# WOMEN &



**Call for action: Ljubljana, CENTR GA - Feb 2020**



# A journey into the uncharted realm of GDPR, PII data sharing and the (impossible?) quest for better, cleaner and true registrant data





# Why?

- December 2019: EURid colleague receives spam & phishing email asking to click a link to verify its ING bank identity.

Similar example,  
some weeks older,  
via SMS and with  
another domain



# Why?

- December 2019: EURid colleague receives spam & phishing email asking to click a link to verify its ING bank identity.
- Involved domain:
  - **ing-betaalverzoek.ccTLD** (= “ING payment request” in Dutch)

# Why?

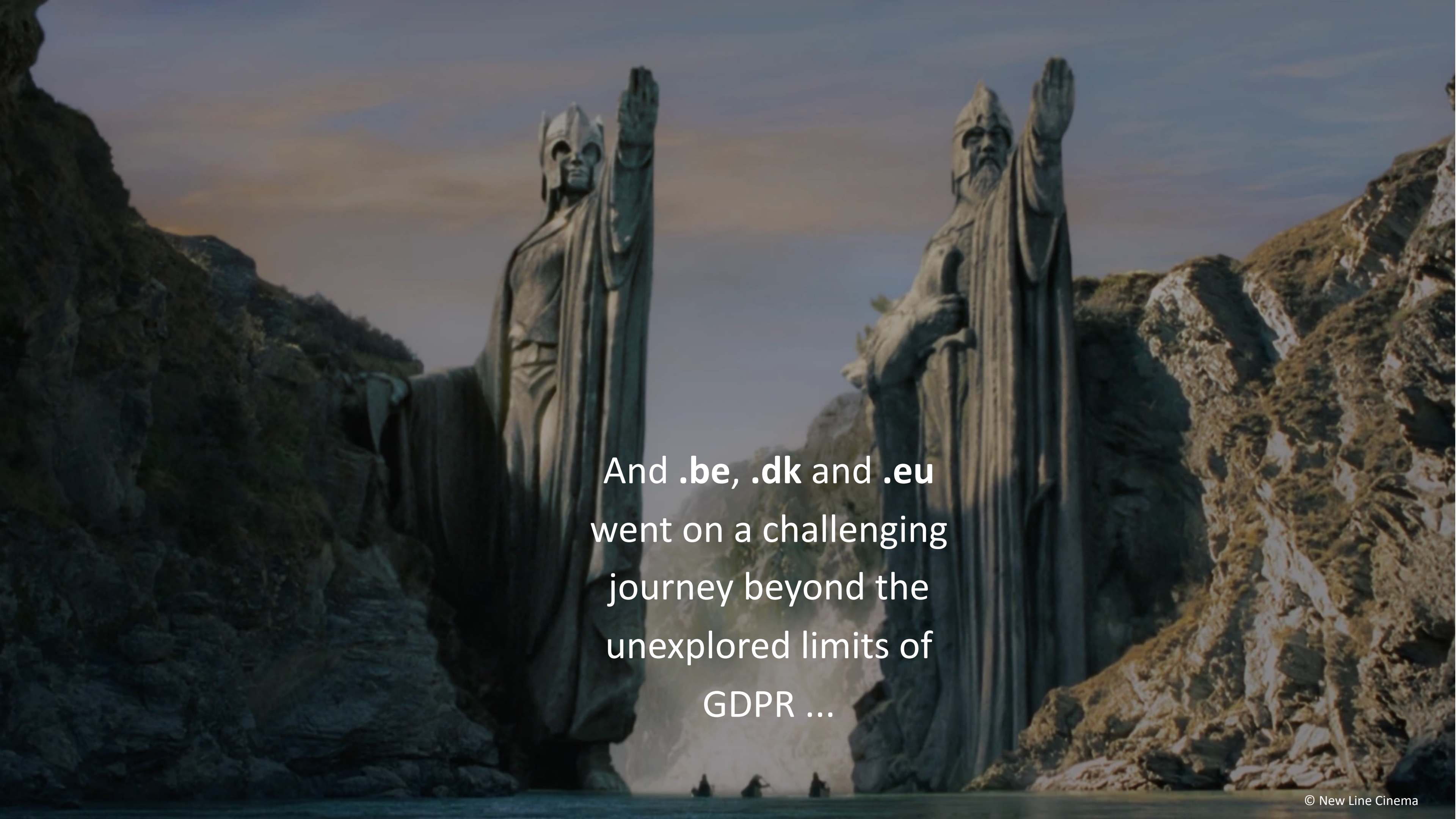
- December 2019: EURid colleague receives spam & phishing email asking to click a link to verify its ING bank identity.
- Involved domain:
  - **ing-betalverzoek.ccTLD** (= “ING payment request” in Dutch)
- 3 and 4 days later we detect registration of:
  - **ing-betalverzoek.eu & ing-betaaiverzoek.eu**
  - Apparently correct registration data from 2 “different” Registrants
  - We could miss them at pre-delegation checks → may enter the zone

# Outcome

- EURid found these domains because we are actively looking for abuse\*. eg: bank, financial and ID theft scams.
- But we may miss other allegedly abusive registrations
- We are interested in receiving alerts from other TLDs
- Would you like to share and/or receive this alerts?
- Or should we just inform our national CSIRT ?

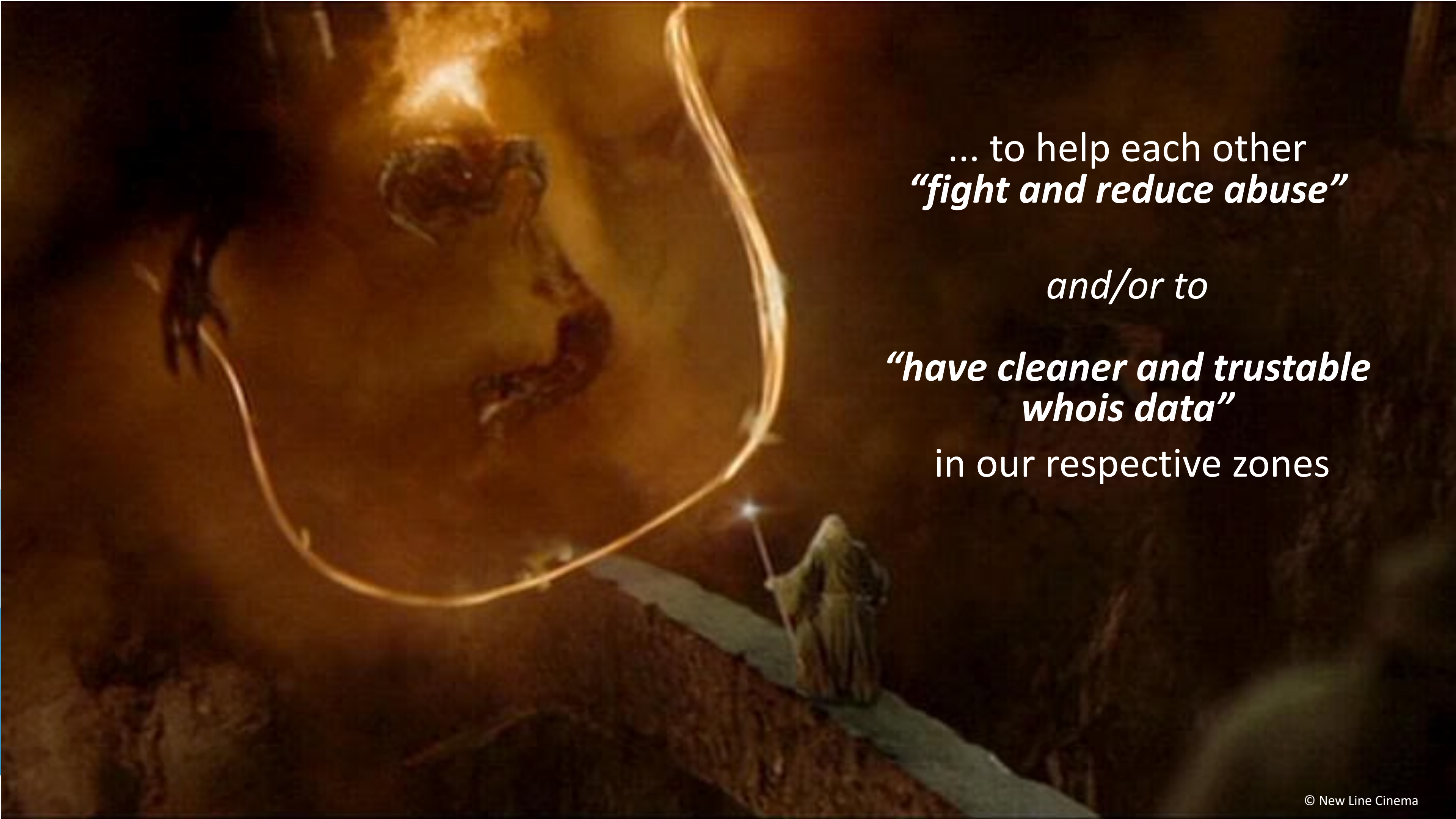
**\*Abuse:**  
“Web sites or domains we would not recommend to our family and friends”



The image features two massive, weathered stone statues standing on a rocky shore. The statue on the left is a woman with a crown and a long, flowing robe, her right hand raised. The statue on the right is a man with a long white beard, wearing a hooded robe and holding a staff, with his right hand raised. The background shows a rugged, rocky coastline under a sky with soft, golden light, suggesting dawn or dusk. In the distance, a few small figures can be seen on the water.

And **.be**, **.dk** and **.eu**  
went on a challenging  
journey beyond the  
unexplored limits of  
GDPR ...





... to help each other  
***“fight and reduce abuse”***

*and/or to*

***“have cleaner and trustable  
whois data”***

in our respective zones



... to help each other  
***“fight and reduce abuse”***  
or to

***“have cleaner and trustable  
whois data”***  
in our respective zones

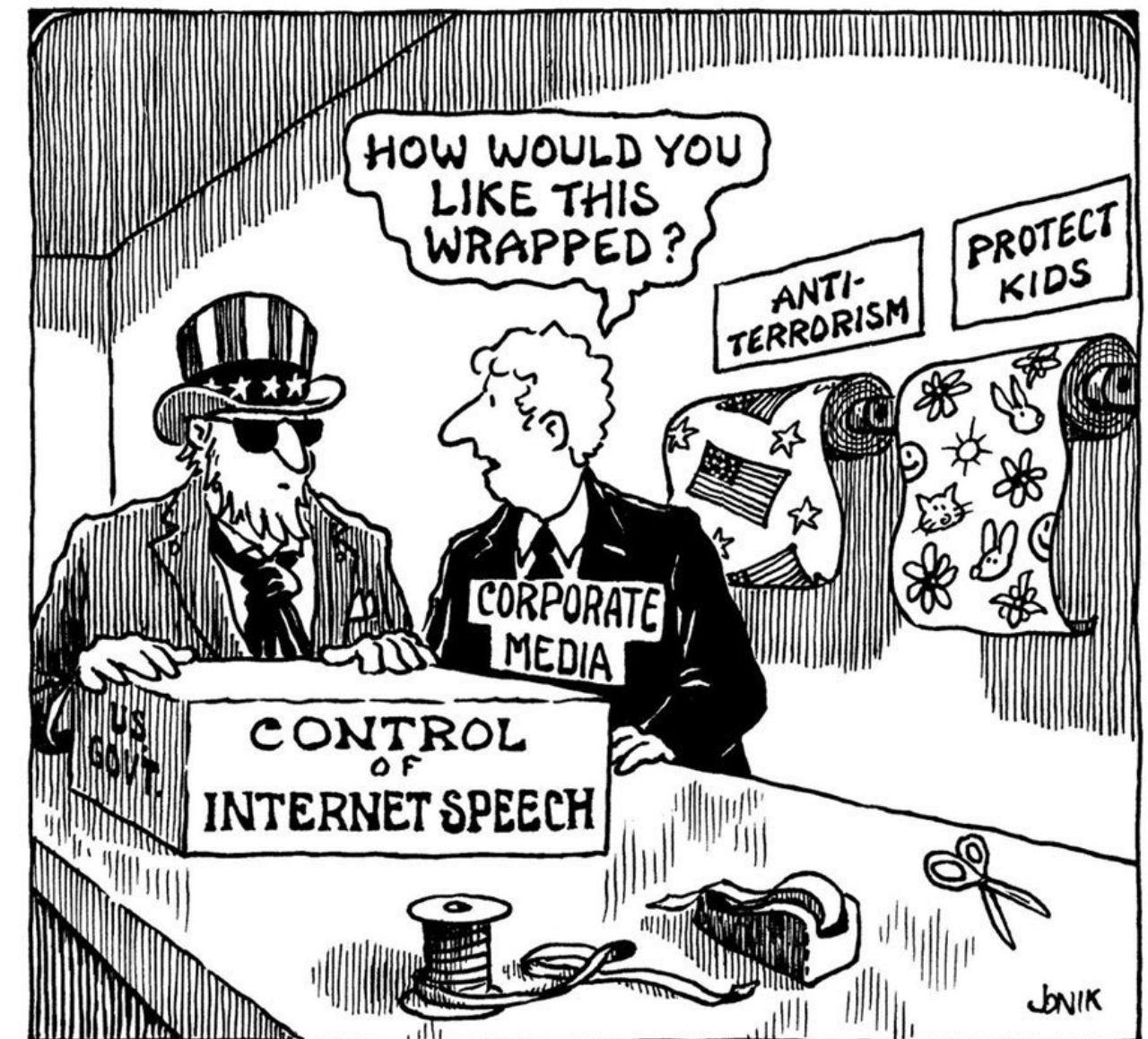
Abusive or  
malicious  
registrations

You shall  
not pass!

.be, .dk, .eu

# As well as

- To have a better and valid whois data base  
- KYC
- To offer a safer zone and help our customers and users - TRUST
- To be proactive and influence decision making before being forced to follow other's rules decided w/o our participation

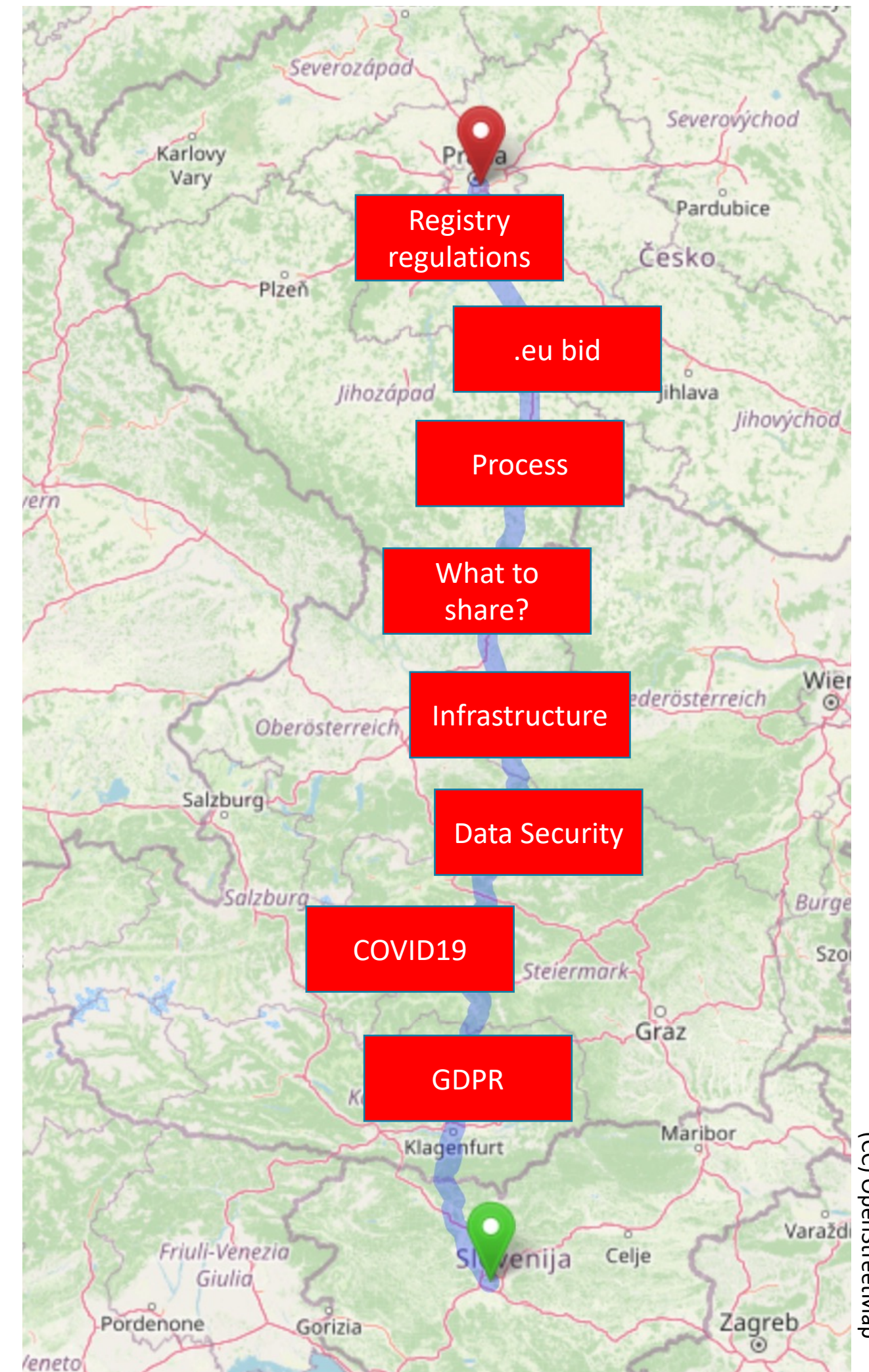


© John Jonik



# Abuse prevention: Sharing indicators task force

- From **Ljubljana**  
CENTR GA - Feb 2020
- To **Praha**  
CENTR Jamboree - May 2022



# Where are we now?

dnsbelgium

.dk hostmaster

eu  
Powered by EURid

- Start small, suffer learning curve → .be, .dk, .eu
- Then, share with ICANN members for comments and learnings from others doing similar things WW
- Open it to CENTR EU GDPR abiding members that will like to join (WiP)

We are here



# Where are we now?

- ✓ Discussed and re-defined goals and scope
- ✓ Studied GDPR impact and possibilities
  - ✓ data sharing, retention, owner, processor, ...
- ✓ Defined an **easy** and **decentralized** data sharing infrastructure
- ✓ Signed cooperation agreement
- ✓ Ready to start sharing data and measure results
-  We will report back in some months about pros, cons and more learnings and open it to other ccTLDs.

# How does it work?

- On a totally voluntary basis
- Decentralized system
- Collective intelligence by sharing data
- Guidelines: privacy by design + privacy by default
- Each registry **offers** what it thinks it is relevant to identify suspicious registrations (minimize)
- Each registry **takes** what it thinks it may need to complement its detection capabilities

*"be cautious in what you share (GDPR!),  
be conservative in what you accept from others"*



# How does it work?

- Process and data security (PGP, accounts, logs, firewall, ...)
- Despite that in too many suspicious cases, data may look formally OK but be totally useless and not connected to the registrant
- GDPR mind-set
  - Share only what's strictly necessary to detect issues (+ no drowning in data)
  - Not obliged to accept what others offer you (set your own level of comfort)
  - Regularly delete collected data

Tired!

Wired!

# From “abuse” to “data accuracy”

At pre-delegation or in the first hours after domain delegation:



Difficult to state  
“abusive domain”



Easier to state  
“abusive or malicious registration”



# From “abuse” to “data accuracy”

Tired!

Wired!

- If you detect abuse based on content (counterfeit, pharma, phishing, ...), it's ok but you are too late! (*unless you crawl and check really often*)
- And in many cases only cybersec experts can state maliciousness (malware, botnets, spam, etc)

# From “abuse” to “data accuracy”

Tired!

Wired!

- **We focus on registration data accuracy and risk prevention**
  - Primary effect → fulfil our mission regarding Whois data
  - Secondary effect → less abuse



# From “abuse” to “data accuracy”

Tired!

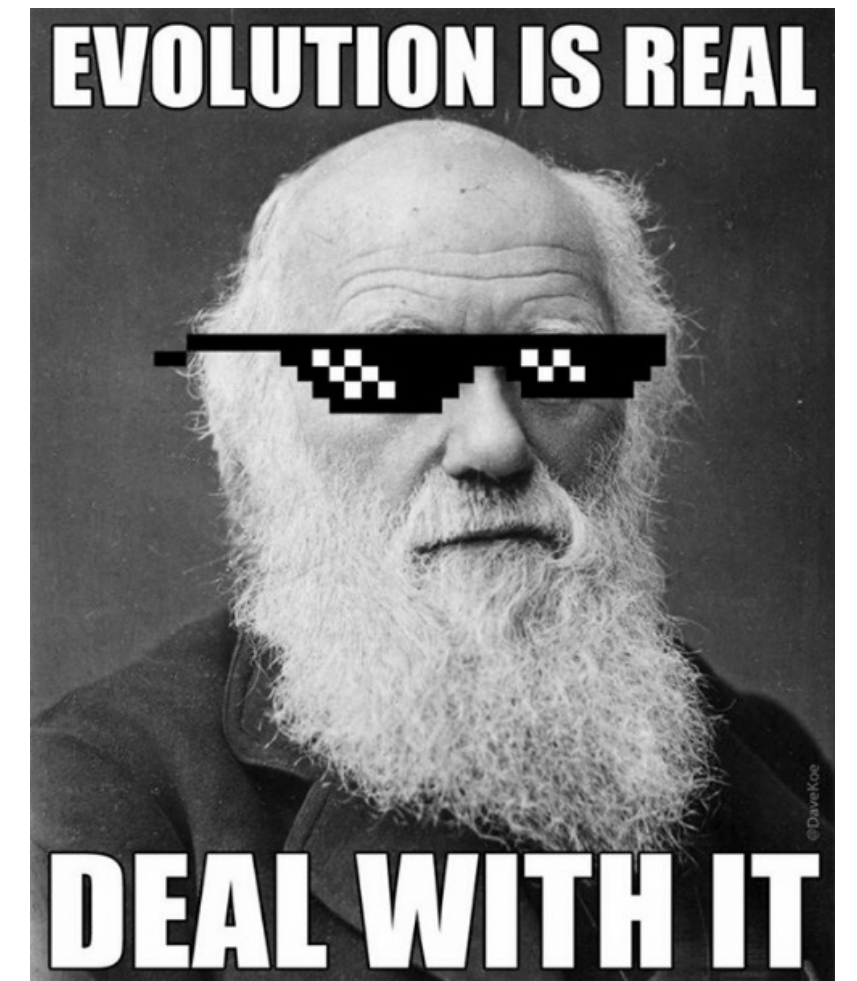
Wired!

- **We focus on registration data accuracy and risk prevention**
  - Primary effect → fulfil our mission regarding Whois data
  - Secondary effect → less abuse

**Delayed effect** → more false but apparently valid registration data (unless KYC)

The more **daring abusers will adapt** with new strategies

**Registries can cooperate** helping each other detecting malicious registrations



How does it work?





# High level process overview

## Pre-delegation checks (APEWS)

- Suspicious registrations → delayed delegation + KYC e-checks
- Otherwise, delegated and is DN added to the zone



# High level process overview

## Post-delegation checks

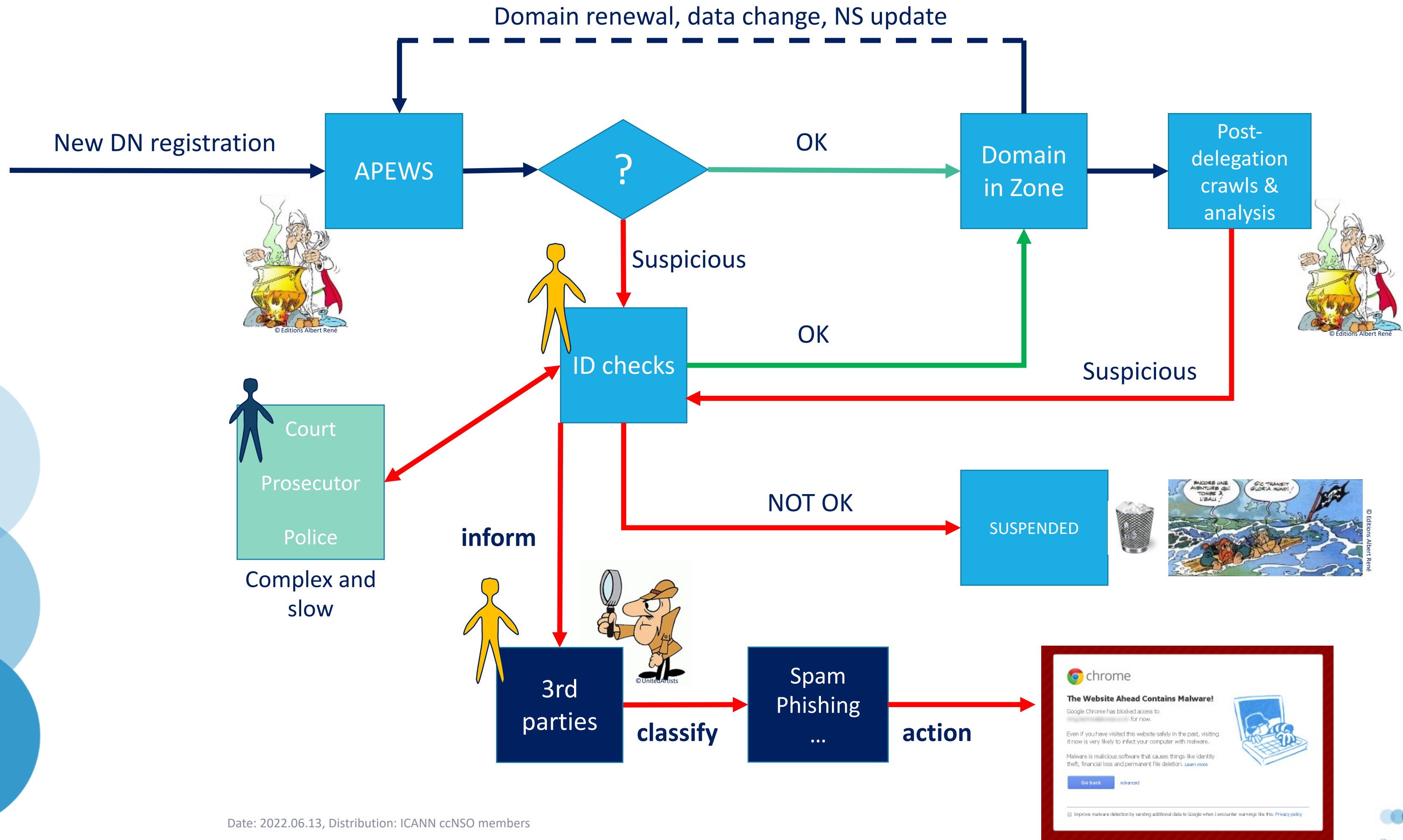
- DN + Registry data + Crawl data + *magic data brewing*
- Human review of reports (2<sup>nd</sup>-check + learn)
- Ry *WhoisQuality* process → KYC + eIDAS + etc
- Share data with partners:
  - of alleged suspicious domain names or weird registrations
  - today, only domain names (DN, NS, MX, Redirect)



**Alleged suspicious  
domain names**







# .be, .dk, .eu Task Force

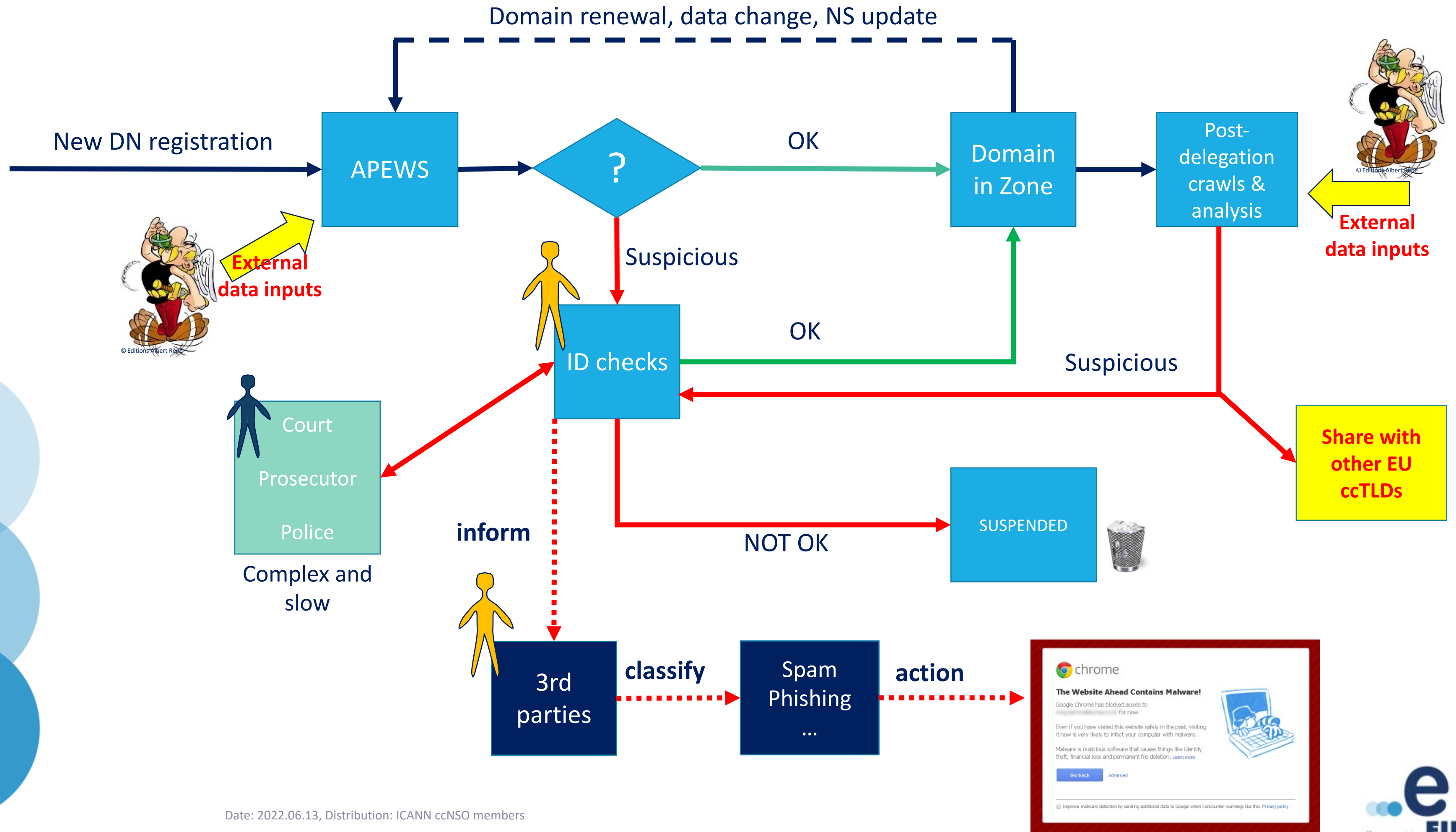
- Which other data points, beyond domain names, are relevant?
- Can we share them with CyberSec partners & LEA too?
- How does GDPR apply in these cases?



# Can we share more than just a domain name?

For instance...

- Domain name
- Email provider & user name
- Registration hour
- Registrar
- Domain target of redirection
- NS name, IP, geoloc (country code)
- MX name, IP, geoloc (country code)
- ASN name or number
- Other?





# Next steps

- Set up distributed infrastructure (each registry its own)
- Start exchanges
- Measure impact
- Propose and implement improvements
- Welcome other GDPR abiding ccTLDs

# Thanks! Questions?

Jordi.iparraguirre@eurid.eu

...eu ...eю ...ΕU

Powered by **EURid**

