# The UN, the EU, and your Business, what comes next?

Elena Plexida
Veni Markovski

20 July 2021

ICANN

# Today's Speakers

**Elena Plexida**

Vice President, Government and IGO Engagement
Elena.plexida@icann.org

**Veni Markovski**

Vice President for UN Engagement
Veni.markovski@icann.org

**Naela Sarras**

Vice President, Global Stakeholder Engagement, North America
Naela.sarras@icann.org

# Updates on Legislative Developments in Europe

Elena Plexida, VP Government and IGO Engagement

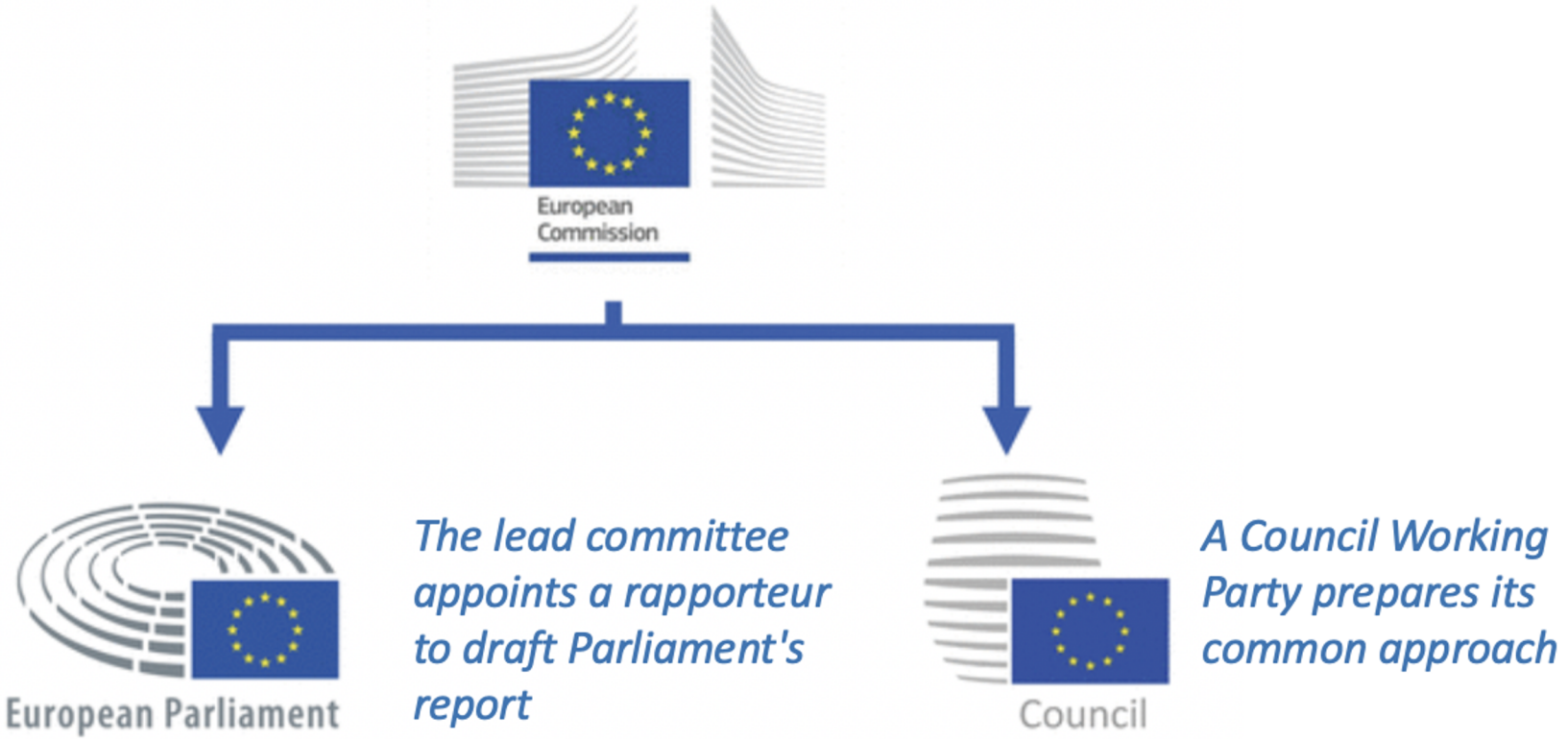
20 July 2021

# Agenda

- EU Legislative Developments
  - NIS 2
  - DSA
- Second Additional Protocol to the Convention on Cybercrime

# NIS2
# The legislative procedure

# Where do we stand process-wise?




The Proposal will be subject to negotiations between the co-legislators, notably the Council of the EU and the European Parliament.

Once the proposal is agreed and consequently adopted, Member States will have to transpose the NIS2 Directive within 18 months.

# NIS2
# The scope as regards the DNS

# The DNS in the context of the NIS2 Directive

- NIS2 will impose updated requirements on "essential" and "important" service providers in critical sectors. Companies are defined as either “essential” or “important”, with different sets of obligations.
- NIS2 applies “*to all providers of DNS services along the DNS resolution chain, including operators of root name servers, TLD name servers, authoritative name servers for domain names and recursive resolvers*” (rec 15).
- They qualify as essential services, while there is no identification system by the EU Member States.
- Territorial scope similar to the GDPR: A DNS service provider must designate a representative under NIS2, in cases in which a DNS service provider not established in the EU offers services within the EU (cf. Art. 24 (3) NIS2)
- Moreover, the small and micro business exemptions do not apply to TLD name registries and DNS service providers (cf. Art 2 (2) NIS2)

# The DNS in the context of the NIS2 Directive

- Main responsibilities for essential services under the NIS2 Directive are:

  - Implementation of appropriate and proportionate technical and organisational measures (Art. 18 NIS2)
  - Reporting obligations (Art. 20 NIS2)
  - Provide contact details for the registry of essential entities to ENISA (Art. 25 NIS2)

# The DNS in the context of the NIS2 Directive

- Implementation of appropriate and proportionate technical and organisational measures (Art. 18 NIS2)

*With regard to the state of the art, implementation of appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which used in the provision of services, including at least the following:*

- *Risk analysis and information system security policies;*
- *Incident handling (prevention, detection, and response to incidents);*
- *Business continuity and crisis management;*
- *Supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services (thereby taking into account the vulnerabilities specific to each supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures);*
- *Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;*
- *Policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures;*
- *The use of cryptography and encryption.*

# The DNS in the context of the NIS2 Directive

- Reporting obligations (Art. 20 NIS2)

*Essential entities must notify without undue delay:*

1. *The competent authorities or the established computer security incident response teams (CSIRT) of any incident having a significant impact on the provision of their services;*
   - *An incident is significant if:*
     - *The incident has caused or has the potential to cause substantial operational disruption or financial losses for the entity concerned; or*
     - *The incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses.*
   - *Initial notification within 24 hours (where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action)*
   - *Final report within 1 month, including at least*
     - *Detailed description of the incident, its severity and impact;*
     - *The type of threat or root cause that likely triggered the incident;*
     - *Applied and ongoing mitigation measures.*
2. *Where appropriate the recipients of their services of incidents that are likely to adversely affect the provision of that service;*
3. *The competent authorities or the CSIRT of any significant cyber threat identified that could have potentially resulted in a significant incident;*
4. *The recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat and where appropriate also of the threat itself.*

# The DNS in the context of the NIS2 Directive

- Provide contact details for the registry of essential entities to ENISA (Art. 25 NIS2)

*Within 12 months after entering into effect of the NIS2 Directive important and essential entities must submit the following information to ENISA:*

- *Name of the entity;*
- *Address of its main establishment and its other legal establishments in the EU or, if not established in the EU, of its representative designated; and*
- *Up-to-date contact details, including email addresses and telephone numbers of the entities*

*Notify ENISA about any changes to the details submitted without delay, and in any event, within 3 months from the date on which the change took effect.*

# The DNS in the context of the NIS2 Directive

- Sanctions

  There may also be sanctions for important and essential entities that fail to meet these responsibilities. For non-compliance with Art. 18 and 20 NIS2 EU Member States are required to implement potential **maximum fines** of at least EUR 10 Mio. or 2 % of the total worldwide annual turnover of the undertaking to which the important/essential entity belongs in the preceding financial year, whichever is higher.

# Amendments by the Parliament rapporteur

Recital 15

(15) Upholding and preserving a reliable, resilient and secure domain name system (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. Therefore, this Directive should apply to ~~all providers of DNS services along the DNS resolution chain, including operators of root name servers,~~ top-level-domain (TLD) name servers, ***recursive domain name resolution services for internet end-users and*** authoritative domain ***name resolution services as a service procurable by third-party entities*** ~~authoritative name servers for domain names and recursive resolvers~~.

Article 4 – paragraph 1 – point 14

(14) 'DNS service provider' means an entity that provides ~~recursive or authoritative domain name resolution services to internet end-users and other DNS service providers~~***:***
***(a)*** recursive domain name resolution services to internet end-users***; or***
***(b) authoritative domain name resolution services as a*** service ***procurable by third-party entities***;

# NIS2
# Provisions related to registration data

# Provisions related to registration data

**Article 23 "Databases of domain names and registration data"** of NIS2 would require EU Member States to ensure that domain name registries take several actions related to registration data:

- collect and maintain accurate and complete domain name registration data in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data.
- ensure that the databases of domain name registration data contain relevant information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs.
- have policies and procedures in place to ensure that the databases include accurate and complete information and that such policies and procedures are made publicly available.
- publish, without undue delay after the registration of a domain name, domain registration data which are not personal data.
- provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law; reply without undue delay to all requests for access; make policies and procedures to disclose such data publicly available.

# Provisions related to registration data

Recital 59

(59) Maintaining accurate***, verified*** and complete databases of domain names registration data (so called 'WHOIS data') is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. ***In order to ensure the availability of accurate, verified and complete domain name registration data, TLD registries and entities providing domain name registration services should be required to collect domain name registration data. They should aim to ensure the integrity and availability of such data by implementing technical and organisational measures, such as a confirmation process for registrants. In particular, TLD registries and entities providing domain name registration services should establish policies and procedures for the collection and maintenance of accurate, verified and complete registration data, as well as for the prevention and correction of inaccurate registration data.*** Where processing includes personal data such processing shall comply with Union data protection law.

# Provisions related to registration data

Article 2 – paragraph 6 a (new)

***6a. Essential and important entities, CERTs, CSIRTs and providers of security technologies and services, shall process personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, to meet the obligations set out in this Directive. Where this Directive requires the processing of personal data for the purpose of cybersecurity, including for contributing to the security, stability and the resilience of the DNS, that processing is considered to be necessary for compliance with a legal obligation as referred to in point (c) of Article 6(1) of Regulation (EU) 2016/679. For the purpose of Articles 26 and 27 of this Directive, processing, as referred to in point (f) of Article 6(1) of Regulation (EU) 2016/679, is considered to be necessary for the purposes of the legitimate interests pursued by the essential and important entities.***

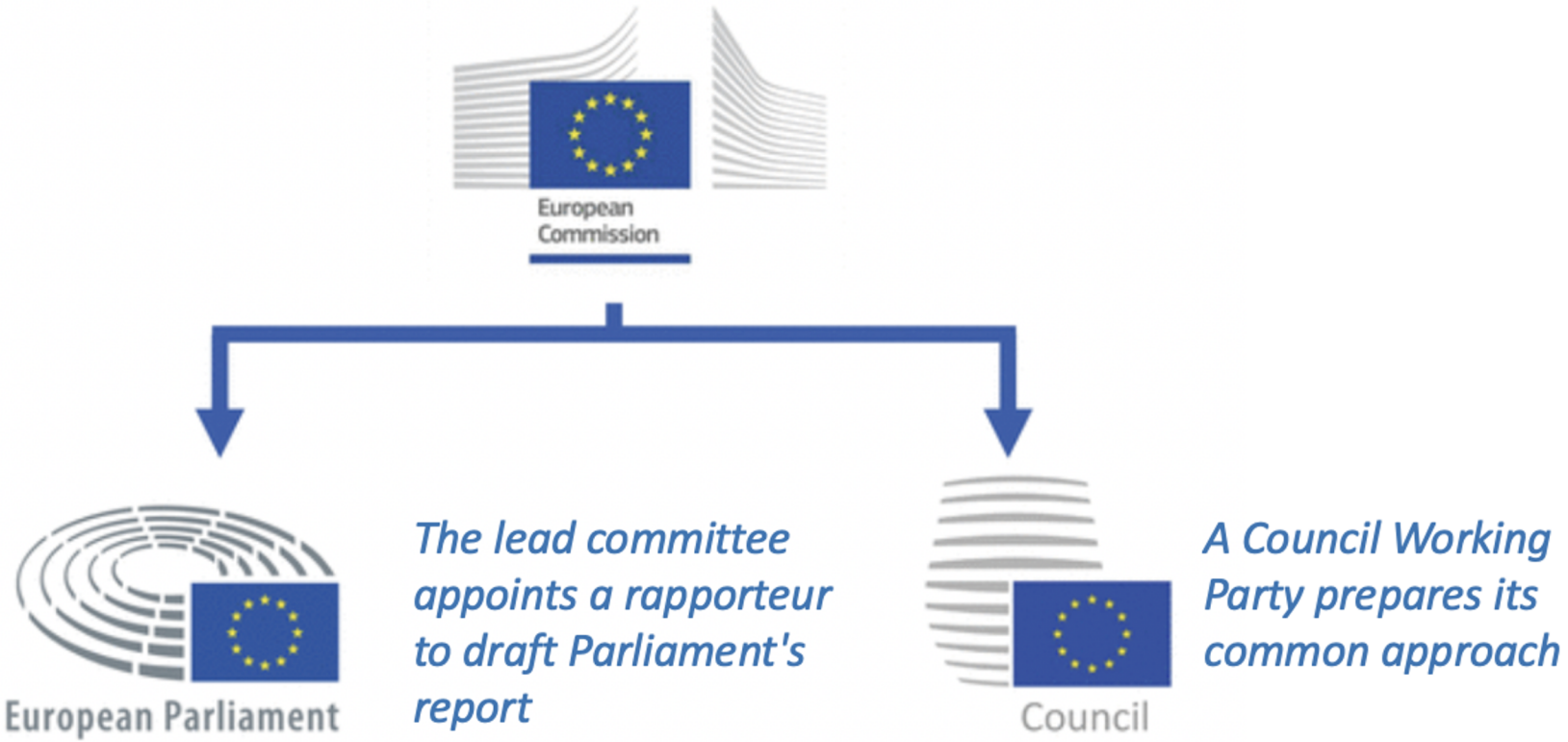
# Provisions related to registration data

Article 4 – paragraph 1 – point 15 a (new)

***(15a) 'domain name registration services' means services provided by domain name registries and registrars, privacy or proxy registration service providers, domain brokers or resellers, and any other services which are related to the registration of domain names;***

# DSA update

# Where do we stand process-wise?




The Proposal will be subject to negotiations between the co-legislators, notably the Council of the EU and the European Parliament.

# The Digital Services Act

The Digital Services Act (DSA) introduces new EU-wide obligations addressing intermediary services' handling of illegal online content.

It also attempts to clarify the rules on liability and to create incentives for proactive measures.

***Noteworthy regulatory aspects:***

- *Exterritoriality effect*
- *Does not specify "illegal content"*

# The Digital Services Act: scope

## Cumulative due diligence obligations

| OBLIGATIONS | VERY LARGE PLATFORMS | ONLINE PLATFORMS | HOSTING SERVICES | ALL INTERMEDIARIES |
|---|---|---|---|---|
| Points of contact | • | • | • | • |
| Legal representatives | • | • | • | • |
| Terms and conditions | • | • | • | • |
| Transparency reporting | • | • | • | • |
| Notice & Action | • | • | • | |
| Statement of reasons | • | • | • | |
| Complaint handling | • | • | | |
| Out of Court Dispute Settlement | • | • | | |
| Trusted flaggers | • | • | | |
| Abusive behaviour | • | • | | |
| Know Your Business Customer (KYBC) | • | • | | |
| Reporting criminal offences | • | • | | |
| Advertising transparency | • | • | | |
| Additional transparency reporting | • | • | | |
| Risk assessment and mitigation | • | | | |
| Independent audits | • | | | |
| Recommender systems | • | | | |
| Enhanced advertising transparency | • | | | |
| Data access and scrutiny | • | | | |
| Compliance officer | • | | | |
| Enhanced Transparency reporting | • | | | |

→ Cumulative obligations

# Why Do We Care?

Recital 27:

*"...providers of services establishing and facilitating the underlying logical architecture and proper functioning of the internet, including technical auxiliary functions, can also benefit from the exemptions from liability set out in this Regulation,* ***to the extent that their services qualify as "mere conduits", "caching" or hosting services. Such services include, as the case may be,*** *wireless local area networks,* ***domain name system (DNS) services, top–level domain name registries****,…"*

**★Registries, registrars and potentially ICANN org could possibly fall under the general scope of application of the DSA as "intermediary services"**
**★There is ambiguity on whether they would also qualify for the DSA exemption from liability**

# New Provisions on Traceability of business users

The European Parliament rapporteur's draft report on the DSA has been published.

The rapporteur has added a new article (13b) to **enhance the principle of identification (know your business customer – KYBC) to all information society services/providers of intermediary services (not limited to platforms as in the Commission proposal). This includes on domain name registries** (the draft report notes "registries" in the justification, maybe just a mistake to omit registrars).

There's no change on recital 27, or the categorization of intermediary services

# Article 13b (new) Traceability of business users

***1. A provider of intermediary services shall ensure that business users can only use its services if the provider of intermediary service has obtained the following information:***

***a)*** ***the name, address, telephone number and electronic mail address of the business user;***

***b)*** ***a copy of the identification document of the business user or any other electronic identification as defined by Article 3 of Regulation (EU) No 910/2014 of the European Parliament and of the Council1a;***

***c)*** ***the bank account details of the business user, where the business user is a natural person;***

***d)*** ***where the business user is registered in a trade register or similar public register, the trade register in which the business user is registered, and its registration number or equivalent means of identification in that register;***

***2. The provider of intermediary services shall, upon receiving that information and until the end of the contractual relationship, make reasonable efforts to assess whether the information referred to in points (a) and (d) of paragraph 1 is reliable and up-to-date through the use of any freely accessible official online database or online interface made available by a Member States or the Union or through requests to the business user to provide supporting documents from reliable sources.***

# Article 13b (new) Traceability of business users

***3. Where the provider of intermediary services obtains indications that any item of information referred to in paragraph 1 obtained from the business users concerned is inaccurate or incomplete, that provider of intermediary services shall request the business user to correct the information in so far as necessary to ensure that all information is accurate and complete, without delay or within the time period set by Union and national law.***
***Where the business user fails to correct or complete that information, the provider of intermediary services shall suspend the provision of its service to the business user until the request is complied with.***

***4. The providers of intermediary services shall store the information obtained pursuant to paragraph 1 and 2 in a secure manner for the duration of their contractual relationship with the business user concerned. They shall subsequently delete the information.***

***5. Without prejudice to paragraph 2, the providers of intermediary services shall only disclose the information to third parties where so required in accordance with the applicable law, including the orders referred to in Article 9 and any order issued by Member States' competent authorities or the Commission for the performance of their tasks under this Regulation.***
***6. The providers of intermediary services shall make the information referred to in points (a) and (d) of paragraph 1 available to the recipients of the service, in a clear, easily accessible and comprehensible manner.***

# Second Additional Protocol to the Convention on Cybercrime

# 2nd Additional Protocol to the Convention on Cybercrime

**Article 6 - Request for domain name registration information**

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, for purposes of specific criminal investigations or proceedings, to issue a request to an entity providing domain name services in the territory of another Party for information in the entity's possession or control, for identifying or contacting the registrant of a domain name.

1. Each Party shall adopt such legislative and other measures as may be necessary to permit an entity in its territory to disclose such information in response to a request under paragraph 1, subject to reasonable conditions provided by domestic law.

1. The request under paragraph 1 shall include:
   a. the date issued and the identity and contact details of the competent authority issuing the request;
   b. the domain name about which information is sought and a detailed list of the information sought, including the particular data elements;
   c. statement that the request is issued pursuant to this Protocol, that the need for the information arises because of its relevance to a specific criminal investigation or proceeding and that the information will only be used for that specific criminal investigation or proceeding; and
   d. the time and the manner in which to disclose the information and any other special procedural instructions.

# 2nd Additional Protocol to the Convention on Cybercrime

**Article 6 - Request for domain name registration information**

4. If acceptable to the entity, a Party may submit a request under paragraph 1 in electronic form. Appropriate levels of security and authentication may be required.

4. In the event of non-cooperation by an entity described in paragraph 1, a requesting Party may request that the entity give a reason why it is not disclosing the information sought. The requesting Party may seek consultation with the Party in which the entity is located, with a view to determining available measures to obtain the information.

4. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance or approval, or at any other time, communicate to the Secretary General of the Council of Europe the authority designated for the purpose of consultation under paragraph 5.

4. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities designated by the Parties under paragraph 6. Each Party shall ensure that the details that it has provided for the register are correct at all times.

# IGOs update

**Developments at the Intergovernmental Organizations**

Veni Markovski
Vice-President for UN Engagement

Zoom call
July 2021

# UN and UN agencies

- **UNGA First, Second and Third Committees deliberations**
  - UN OEWG (second edition, started June 1, 2021)
  - UN GGE (ended May 28, 2021)
  - UN AHC (started work May 10, 2021)
  - And don't forget WSIS+20 negotiations

- **ITU (WTSA, WTPF, WTDC, PP-22)**
  - WTPF: 16-18th of December 2021
  - WTSA: 1 – 9 March 2022
  - Council: 21 – 31 March 2022
  - WTDC: 6 – 15th of June 2022
  - PP: 26th of September to 14th of October 2022

- **Update on the ICANN GE papers:** 007 – Russia country focus paper and 008 – Country Focus Report: The Netherlands and the "Public Core of the Internet"

# UN | ITU Secretary-General Run: Country position

On 21 April 2021, Ernst Chernukhin, Ministry of Foreign Affairs: "...The Russian Federation has been consistently calling for the **internationalization of the management of the Internet**, as well as for increasing the role of governments in this process." He also said, "The Russian Federation, **within the U.N. system**, insists on adopting a number of coordinated measures, including [...] **development at the intergovernmental level of global policies in the area of Internet management**[...] As we see it, the optimal option for this would be **transferring Internet management prerogatives specifically to the ITU**[...] This **strategic objective may be achieved by electing or promoting the Russian candidate** to the position of the ITU Secretary-General in the 2022 elections …**and by holding the 2025 anniversary U.N. IGF** in Russia."

# UN, ITU, etc.

- What happened at the ITU Council (countries positioning themselves already for PP-22)
- UNGA deliberations around ICT for Development resolution
- UN Tech Envoy office
- IGF evolution
- New IP, national legislations, etc.

# Questions?

# Engage with ICANN

## Thank You and Questions

Visit us at **icann.org**
Email: Veni.Markovski@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

soundcloud/icann

instagram.com/icannorg

# Other Virtual Opportunities

- Please join a public webinar hosted by ICANN's Global Domains and Strategy team on "ICANN DNS Security Threat Mitigation Program Update and Community Discussion" on Thursday, 22 July 2021 at 16:00 UTC.
  - For more information and to register, please visit https://www.icann.org/en/announcements/details/webinar-icann-dns-security-threat-mitigation-program-update-and-community-discussion-1-7-2021-en

# Engage with ICANN

## Thank You and Questions

Visit us at **https://www.icann.org/resources/pages/ssad-odp-2021-04-29-en**

Email: **ODP-SSAD@icann.org**

 @icann

 facebook.com/icannorg

 youtube.com/icannnews

 flickr.com/icann

 linkedin/company/icann

 soundcloud/icann

 instagram.com/icannorg