INTERNET
INFRASTRUCTURE
COALITION

i2Coalition EU Tech Handbook

Overview of the state of play

Background

Between September and November 2022, i2Coalition - via our Brussels-based partner Political Intelligence - will provide updates on European policy developments of interest to the Coalition's members. The aim of this exercise is to **improve awareness** of understanding of overseas developments, which often have spillover effects, as well as to start **expanding the Coalition's influence to Brussels**, positioning it as a key expert in matters concerning the Internet infrastructure.

Outlook

The Parliamentary recess (18 July - 26 August) has recently come to an end in Brussels, which presents the right opportunity to take stock of all **ongoing procedures of relevance** to the i2Coalition and its members. It is no secret that the European Union (EU) has been extremely active in the past years in legislating on digital and tech issues, and the overwhelming majority of these laws have an **extraterritorial effect**. As such, they have a direct impact on members offering services to EU customers, as well as an indirect effect of putting pressure on US lawmakers to follow suit. We hope that this upcoming monitoring report series will help to shed light on what's happening in Brussels and to establish an ever-stronger influence on the proceedings overseas.

The aim of this document

This document below has two objectives.

1. On the one hand, it aims to provide a **general 'cheat sheet' on EU policy-making**, a kind of point of reference to turn to when faced with questions regarding the EU's abstruse legislative processes.
2. On the other hand, it presents a **snapshot of the state of play** **regarding the key legislative and non-legislative processes** of relevance to the Coalition, serving as a basis for understanding the upcoming monthly EU reports.

In case you are already familiar with the basics of policy-making in Europe, please feel free to jump to the section detailing the state of play on ongoing EU policy activity.

How does the EU work?

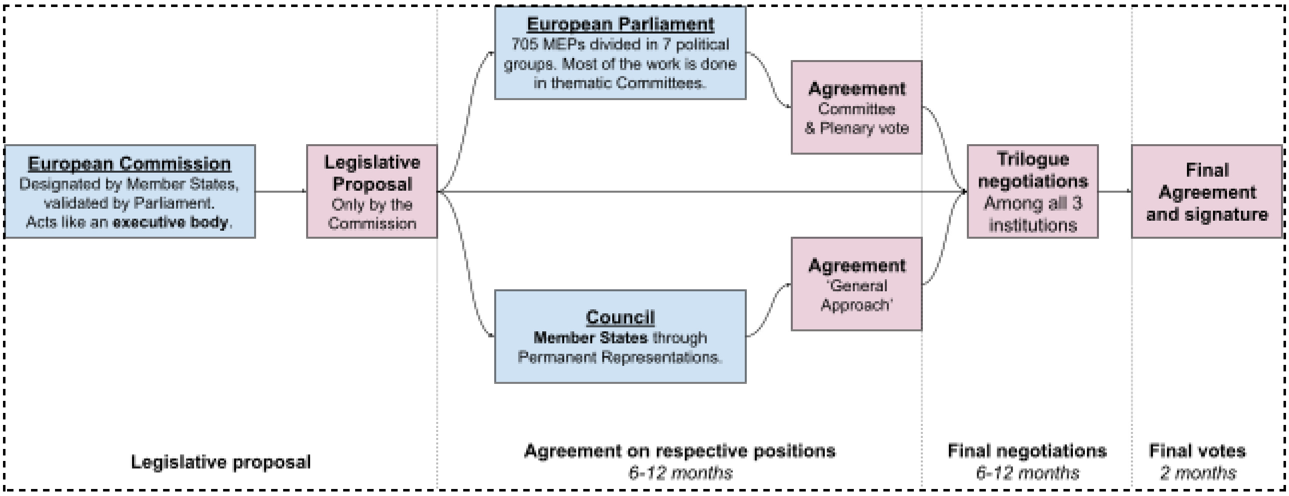
The EU has many institutions and agencies, but overall, it is enough to be familiar with the three main ones - **the Commission, the Parliament, and the Council**. Below, you will find an overview of each of these, as well as their legislative role.

	European Commission	European Parliament	Council of the EU
Similar to *or*	*US President* *Executive body*	*US House* *Lower house*	*US Senate* *Upper house*
Represents	The Union	EU Citizens	The Member States
Consists of	28 Commissioners, 33 Directorates-General, 32,000 civil servants	705 directly elected Members (MEPs) in 23 specialized Committees	Member State representatives (6-months rotating presidency)
Legislative role	Can propose law, but has no say in the final text	Cannot propose law, but can propose changes	Cannot propose law, but can propose changes

The EU legislative process

The **enactment of an EU legislation takes around 24 months** on average (from first proposal to final agreement). Contrary to the US, in the EU **only the executive** (European Commission) **can propose laws**, therefore almost all published proposals actually end up becoming law, although usually only after undergoing considerable changes. Once a law is proposed, there are two main distinct periods, each taking around 6-12 months:

1. **Adoption of the respective negotiating positions** of the Council (representing Member States) and the Parliament (representing citizens);
2. **Tripartite so-called 'Trilogue' negotiations**, where the two aforementioned institutions try to build a mutually acceptable final text. The Commission (which drafted the original proposal) only acts as an 'honest broker' between them.

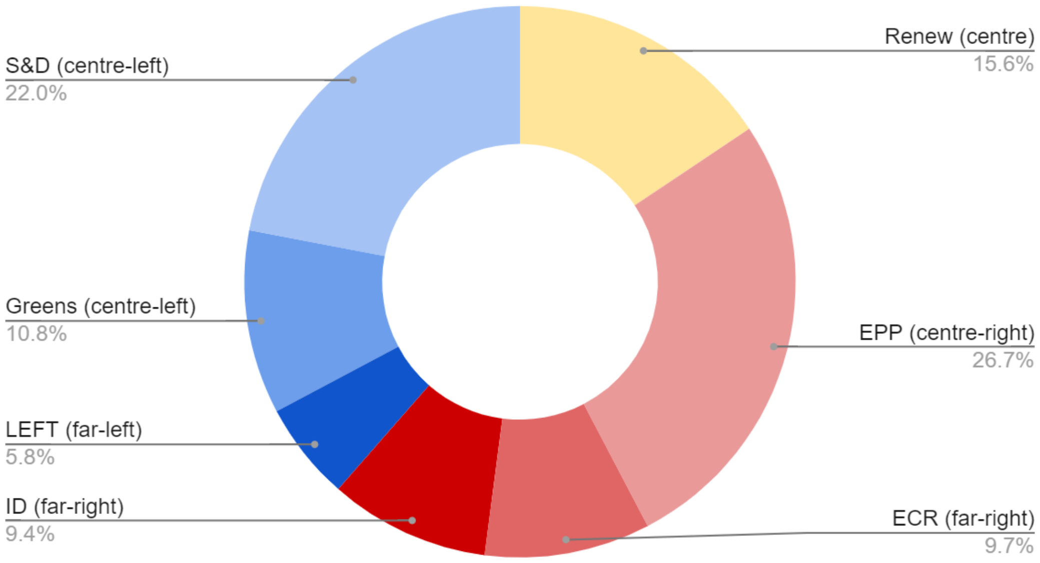

European Commission
Designated by Member States, validated by Parliament. Acts like an executive body.
Legislative Proposal
Only by the Commission
European Parliament
705 MEPs divided in 7 political groups. Most of the work is done in thematic Committees.
Agreement
Committee & Plenary vote
Council
Member States through Permanent Representations.
Agreement
'General Approach'
Trilogue negotiations
Among all 3 institutions
Final Agreement and signature
Legislative proposal
Agreement on respective positions
6-12 months
Final negotiations
6-12 months
Final votes
2 months

Good to know: EU acts can take two distinct forms: Regulations, which contain explicit rules and are **directly applicable** in Member States; and Directives, which leave more room for Member States, as they need to be **transposed into national legislation** (thereby often leading to differing interpretations among Member States).

Political dynamics

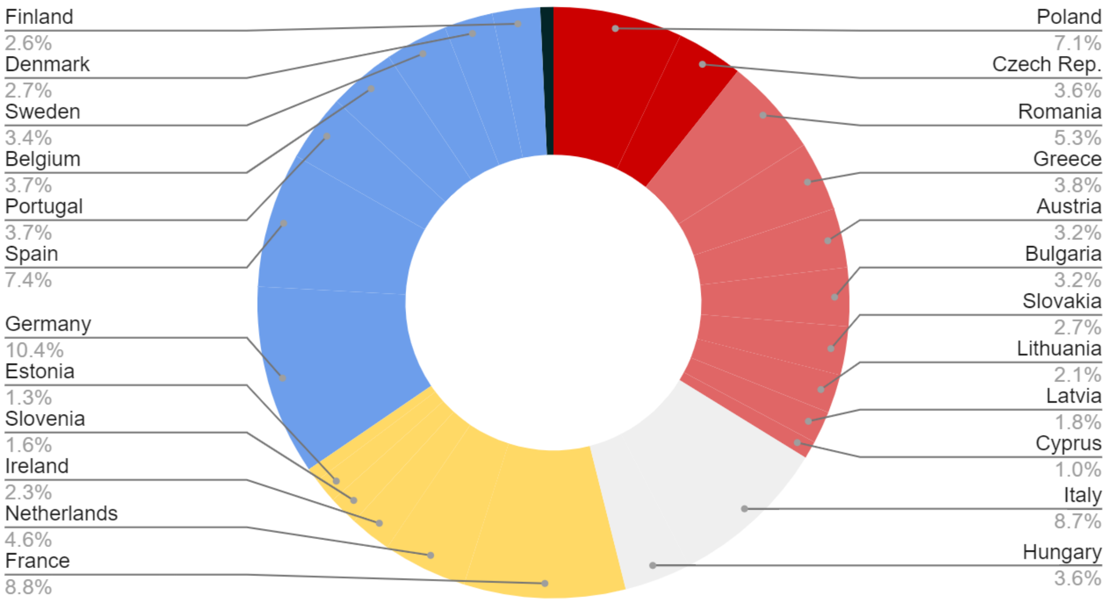
Due to the proportional representation, power dynamics in the European institutions are **rather balanced** in both the Parliament and Council (i.e. the governing parties in different Member States). This leads to the necessity of **ad-hoc alliances around specific topics**. As a consequence, the majority of the legislative files are **adopted with a broad centrist coalition**, with only the far-left and far-right parties potentially opposing.

Political orientation of parties in the European Parliament



🟦 left-leaning parties ; 🟥 right-leaning parties ; 🟨 centrists; ⬜ other/non-affiliated parties

Member States, their political orientation and voting power



EU files of relevance for i2C

Table of contents

Overview of relevant files

🟩 Finalized legislative procedure; 🟦 Ongoing legislative procedure ; 🟪 Upcoming legislative act ; 🟧 Non-legislative act ; 🟨 Study / Tender (*) Priority

Intermediary liability and content policy	Competition and antitrust	Data policies	Law enforcement	Cybersecurity
🟩 **DSA** Digital Services Act: content moderation and platforms responsibility. (* Intermediary liability)	🟩 **DMA** Digital Market Act: antitrust regulation.	🟦 **ePrivacy** Restrict in-device data usage, "cookie" law. In correlation with GDPR. (* Metadata retention)	🟩 **Terrorist Content Regulation** Preventing the dissemination of terrorist content online. (* Remove terrorist content within one hour)	🟩 **NIS2** Revision of the EU cybersecurity regulation for critical infrastructures.
🟦 **CSAM** Rules to prevent and combat child sexual abuse. (* End of E2EE and content scanning)	🟪 **"Connectivity Infrastructure Act"** (TBC) Force content providers to participate in network fees. (* Cloud/CDN to pay for Internet infrastructure along with telcos)	🟦 **Data Act** Harmonized rules on fair access and use of data. Improve cloud switching for clients. (* Cloud switching)	🟦 **e-Evidence** European Production and Preservation Orders for electronic evidence in criminal matters. (* Data access under 10 days)	🟦 **eIDAS Revision** Rules for trust services and creation of an EU-wide digital identity.
🟧 **EU toolbox against counterfeiting** Cooperation between stakeholders for Intellectual Property (IP) infringements.		🟦 **New EU-US Data Transfer** Replace previous 'Privacy Shield' agreement. (* Data transfer)	🟧 **EU-US law enforcement access regulation** Exchange of personal information for criminal and terrorism puprpose.	🟪 **Cyber Resilience Act** Rules for IoT cybersecurity.
🟨 **Commission's Piracy and Counterfeit Watchlist** List of marketplaces and intermediaries linked to IP infringements.		🟧 **EU Cloud initiatives** European Rulebook, Marketplace and Procurement Rules for cloud.		🟧 **Cybersecurity Certification Scheme** Voluntary cybersecurity programme. The first one aims to provide more security for Cloud providers. (* Sovereignty clause for Cloud)
🟨 **Reports on DNS and TLD abuses** Study on DNS abuses.		🟧 **TTC** EU-US Trade and Technology Council.		🟨 **DNS4EU** Creation of an EU DNS resolver with content filtering. (* DNS competition)

Intermediary liability and content policy

CSAM Regulation

■ Ongoing legislative procedure ■ Regulation 🔗 Legislative text

What is it: The Child Sexual Abuse Material (CSAM) Regulation will introduce harmonized rules for service providers to detect, report and remove child sexual abuse material on their services.

Where do we stand: This legislative procedure has just started and will require another 12-24 months to be adopted and an additional 6-12 months to enter into application.

Next steps		
Start of trilogue negotiations	*Final agreement*	*Entry into force*
~ Q2 2023	~ Q4 2023	~ late 2024

Relevance for i2C:

- Undermining encryption: By seeking to track and intercept illegal content, the proposal could undermine end-to-end encryption (E2EE).
- Obligations on DNS/hosting providers: Although removal is prioritized at the source, it is expected that the proposal will also contain removal obligations for hosting providers and blocking at IP/DNS level as a last resort.

Good to know:

- This recent proposal is a source of **much controversy** already. The main issue is that it obliges service providers to monitor the private communications of users for CSAM, even when those communications are protected via **E2EE** - which many stakeholders point out is not possible with current technology without **introducing backdoors**.
- Moreover, the Commission proposal also tries to tackle *new* CSAM (not part of any hash database) and grooming, both of which require untested **AI/ML technology**. Many stakeholders are worried about the potential **privacy implications** of this, but due to the sensitive nature of the topic, many stakeholders are wary about publicly countering the narrative of the Commission and Child Protection NGOs.
- The incoming DNS4EU initiative will introduce **content filtering** at the DNS level.

Digital Services Act (DSA)

🟩 Finalized legislative procedure ■ Regulation 🔗 Legislative text

What is it: The DSA will introduce new asymmetric obligations (for intermediary services, hosting services, online platform services, and very large online platforms services) on misinformation, dark patterns and online ads.

Where do we stand: The text was definitively adopted by the Parliament last July. The Commission should publish the text in the Official Journal in September. The text will enter into force 20 days after its publication and the rules will be applied 15 months later or in January 2024.

Next steps		
Final EP vote	*Entry into force*	*Compliance*
July 2022	October 2022	January 2024

Relevance for i2C:

- For the first time, intermediaries such as DNS, TLD registrars, and CDNs are explicitly mentioned in a text and benefit from the **exemptions from liability** if they meet specific conditions set out in Articles 3, 4 and 5.
  → *Conditions are along these lines:* the intermediary does not modify the information; the intermediary doesn't have actual knowledge of illegal activities; the intermediary acts promptly to remove the information upon court or administrative order.
- A single regime: new rules will **reduce compliance costs** for intermediaries to avoid 27 different regimes in the Single Market. Note that small and micro companies will be exempted from obligations.
- Hosting services should: provide a single point of contact for illegal content reporting (with actual knowledge, the provider will lose its liability exemption); inform law enforcement of any serious criminal offenses involving a threat to the life or safety of persons designate a legal representative in the EU, and publish an annual report on content moderation.

Good to know:

- Breaching the act can mean heavy fines of up to 6% of global turnover and bans from operating within EU territory.
- Some ideas are circulating in the US to piggyback on the DSA by creating a voluntary mandate based on the EU's digital rules including data access and risk assessment.

EU toolbox against counterfeiting

■ Ongoing non-legislative procedure 🔗 Call for evidence 🔗 EU communication

What is it: The toolbox aims to reinforce the cooperation between relevant stakeholders in the field of intellectual property infringement. The toolbox will clarify the role and responsibilities of each party as well as encourage the sharing of data.

Where do we stand: After a first communication in November 2020, the Commission asked for stakeholders' input early in 2022. The toolbox is set to be published by the end of 2022.

Next steps		
EU communication	*Feedback period*	*Adoption*
November 2020	February 2022	Q4 2022

Relevance for i2C:

- The toolbox will propose new instruments to help stakeholders tackle IP infringements including a "single point of contact"; "new tools [...]to be used by intermediaries" ; and help to coordinate "legal action with right holders".
- Te be monitored. Although the toolkit will not propose any new obligations, it may introduce new mechanisms that will have an impact on the way infringements are handled.

Good to know:

- The legal basis of this text is still being discussed by the Commission based on stakeholders' feedback.
- The text should be in coherence with the Digital Services Act (DSA).

Commission’s Piracy and Counterfeit Watchlist

■ Study / Tender 🔗 2020 watchlist

What is it: The Commission’s Watchlist aims to limit the harm of intellectual property theft and misuse by listing marketplaces and services providers reported by stakeholders.

Where do we stand: The previous Watchlist was published by the Commission in December 2020. The Commission aims to publish a revised version of the list by the end of 2022 based on its Q1 2022 public consultation.

Next steps		
Previous Publication	*Consultation*	*Publication*
December 2020	December - February 2022	End of Q4 2022

Relevance for i2C:

- Debate on the role of CDNs: the 2020 list has reopened the debate on the role of **CDNs** in the fight against online piracy and the importance of their cooperation with authorities. Cloudflare had been mentioned in the list.

Good to know:

- The Piracy and Counterfeit Watchlist is a handy reference and starting point for many media and entertainment industry stakeholders to identify enablers of content distribution across the Union.
- Stakeholders mentioned in this list may be involved in the distribution of illegal content through their supply chain without being legally responsible.
- The list is updated every two years based on stakeholder feedback and the evolution of online piracy techniques.

Reports on DNS and TLD abuses

■ Study / Tender 🔗 Study

→ *In parallel to the legislative process, the EU regularly publishes reports which are used as a basis for the work of policymakers.*

What is it: The DNS abuse Report published last January assesses the scope, impact, and magnitude of DNS abuses, as well as to provide input for possible policy measures on the basis of identified gaps.

Relevance for i2C:

- The study recommends 27 actions that will be used as a working material for future regulations. Therefore, this document is a good starting point for understanding the state of discussion of European officials on the matter.
- Recommendations include generating better **metadata** to identify resources and their attributions to intermediaries; **verification of WHOIS** registration data; allowing IPR holders to preventively block infringing domains; **rewarding TLD registries** with low abuse rates; and forcing usage of **DNSSEC**.

Good to know:

- The EU's Cybersecurity Strategy for the Digital Decade has described DNS as a key part of Europe digital security.
- The EU is working on a sovereign DNS resolver named DNS4EU.
- Three types of abuses were identified: (1) malicious registration of domain names, (2) malicious operations of DNS, (3) distribution of malicious content.

Competition and antitrust

Digital Market Act (DMA)

■ Finalized legislative procedure ■ Regulation 🔗 Legislative text

What is it: The DMA is an antitrust law aimed at reducing the power of core platform services (including online marketplaces, search engines, social networks, operating systems, cloud services and web browsers with a market cap of €75 billion) and improving market access for new players.

Where do we stand: The text was definitively adopted by the Parliament last July. The Commission should publish the text in the Official Journal in September. The text will enter into force 20 days after its publication and the rules will be six months after.

Next steps		
Final EP vote	*Entry into force*	*Compliance*
July 2022	September 2022	Q1 2023

Relevance for i2C:

- Opportunity or obligation: one of the advantages of i2C is the diversity of its members, both in terms of size and sectors. As such, many of its members will see the DMA as a way to gain easier access to the European single market.
- Gatekeepers will have to: refrain from using self-preferencing; stop reusing personal data across platforms (like Facebook / Whatsapp) ; or offer better data portability solutions.

Good to know: In case of non-compliance, gatekeepers face gargantuan fines of up to 10% of their worldwide turnover.

“Connectivity Infrastructure Act”

■ Upcoming legislative act (TBC) 🔗 Commissionaire's interview (FR)

What is it: Following strong telco-lobbying, the European Commission is considering to adopt a legislative act that would somehow push large **content providers** (e.g. Netflix, YouTube) as well as potentially other actors (e.g. Cloud and CDN providers) that make up a large percentage of the traffic on the Internet, to **contribute to the development of network infrastructure**.

Where do we stand: This proposal is only rumored so far. The Commission’s official position is that they see this as the issue and are currently collecting evidence, based on which they may decide to propose a legislative act or not.

Next steps	
Fall 2022	*2023*
Public consultation	Potential proposal (TBC)

Relevance for i2C:

- Costs: Depending on the final agreement, the proposal may introduce obligations for certain providers (e.g. Cloud, CDN) to contribute to telcos based on interest infrastructure usage.
- Imbalance in negotiating power: One of the key objectives of the Commission is to strengthen the power of telcos when negotiating interconnection agreements.

Good to know:

- There is widespread pushback against this idea, with many different actors (Member States, NGOs, content platforms, etc.) warning about unintended potential negative consequences of such an action to net neutrality and the free and open Internet.
- A largely similar discussion already took place in Europe around a decade ago. In that instance, the so-called ‘Body of European Regulators for Electronic Communications’ (BEREC), which consists of national telecom regulators, have concluded in 2012 that such a ‘sending party network pays’ (SPNP) paradigm shift is not justified. Five years later, the Body reiterated that no regulatory intervention is justified for this purpose. Now that the debate has arisen again, BEREC has once again started a workstream to analyze whether it would be justified for them to revise these previous conclusions. In the coming months, they are expected to organize several closed workshops and fact-finding exercises and produce report(s) on their conclusions. Should BEREC once again speak out against this idea, it would become difficult for the Commission to maintain this idea.

Data policies

European Data Act

■ Ongoing legislative procedure ■ Regulation 🔗 Legislative text

What is it: This regulation will facilitate the sharing and reuse of data which are generated by IoT objects with data subjects (consumers, businesses, public sector).
It will also facilitate switching between cloud service providers and regulate circumstances in which the public sector can request data from the private sector for reasons that are of public interest.

Where do we stand: This procedure is still in a relatively early stage as the European Parliament and the Council have to develop their positions on the legislation to come to an agreement. The first opinions are yet to be expressed in the Parliament, and initial comments have recently been made in the Council.

Next steps		
Final agreement	*Entry into force*	*Entry into application*
Q3-Q4 2023	Q4 2023	Q4 2024

Relevance for i2C:

- Impact on Cloud Service Providers**:** Cloud Service Providers will immediately be affected by the cloud switching provisions, for example on the gradual prohibition on egress fees, short portability timelines as well as new interoperability requirements.
- International data transfers: The Data Act introduces limitations on international data transfers. It requires data processing service providers to take all ‘reasonable legal, technical, and organizational measures’ to prevent the international transfer of government access to non-personal data held in the EU that would conflict with European or national laws.
- B2C/B2B data sharing: The Data Act aims to foster the flow of non-personal data (especially IoT) by putting the consumer in charge of it, and allowing them to share it with other companies (e.g. providers of aftermarket services). It, therefore, mandates B2B data sharing, obliging data holders to make data available to a data recipient on fair, reasonable, and non-discriminatory (FRAND) terms.
- B2G data sharing: Companies will be obliged to share data with Member States and the EU in case of - rather broadly defined - ‘exceptional need’.

Good to know: This legislation is part of the ‘European Strategy for Data’ proposed in 2020, of which the earlier adopted Data Governance Act (DGA) and the Data Spaces that are still in development are also a part. The DGA aims to facilitate the re-use of public sector data, and the Data Spaces aims to create one single-market for data in the EU by creating sector-specific legislation for data sharing.

EU Cloud Initiatives

■ Ongoing non-legislative procedures 🔗 Marketplace study 🔗 EU Communication

What is it: Several initiatives, among which are the European Rulebook, Marketplace, and Procurement Rules for the cloud. They are part of a concerted effort by the European Commission to lay down standardized rules for cloud services (thereby increasing their uptake by EU companies), but many of them also contain **'digital sovereignty'** aspects that discriminate against foreign companies in both direct and indirect ways.

Where do we stand: There are several procedures here occurring simultaneously. When looking at them as a whole, all initiatives are expected to kick off during the next 6 months.

Next steps		
Cloud Marketplace	*Cloud Rulebook*	*Procurement rules for Cloud computing in the public sector*
Q4 2023	Q4 2023	Q4 2023

Relevance for i2C:

- Sovereignty provisions**:** Several references to sovereignty have been made. In general, the EU aims to enhance the European Cloud Market with actors like OVH and Orange and is unfavorable of US Cloud Service Providers like AWS, Google Cloud, and Microsoft Azure.
- Cloud Rulebook: This should become one place where all cloud rules come together (right now they are rather scattered e.g. CISPE Handbook, ISO standards, EU Cloud CoC, EU cloud cybersecurity certification scheme).
- Cloud Marketplace: This marketplace would be built on the Rulebook. Cloud Service Providers will be able to offer their services and products there, and potential customers will see which of the different aspects of the Rulebook providers comply with.

Good to know: Discussion on these initiatives mostly happens in technical meetings held behind closed doors, which on the one hand makes it difficult to follow the developments, and on the other hand allows for Member States with strong sovereignty/protectionism agendas (e.g. France) to push political points in otherwise purely technical discussions (see also the example of the EU Cloud Certification Scheme).

New EU-US Data Transfer Framework

■ Ongoing legislative procedure ■ Adequacy decision 🔗 EU Communication

What is it: Third attempt to establish a trans-Atlantic data transfer framework between the United States and the EU. The agreement intends to replace the previous 'Privacy Shield' agreement which was invalidated by the European Court of Justice in July 2020.

Where do we stand: Following the announcement of the agreement 'in principle', the Commission is waiting for the Biden administration to propose the Executive Order that would serve as the cornerstone of the agreement. Once the US commitments are published, the Commission will propose the legislative act to establish the framework. Thankfully, this act would be adopted under so-called secondary (delegated) legislation, which means that it will only take several months to be adopted, instead of the normal 1-2 years for primary legislative acts.

Next steps	
US Executive Order	*Official adoption and entry into force*
Q3 2022	Q1-Q3 2023

Relevance for i2C:

- The solution to the legal uncertainty over EU-US data transfers**:** Following the so-called 'Schrems II' judgment which invalidated the Privacy Shield data transfer framework, any US company transferring EU citizens' data overseas faces compliance risk. This is especially true for tech companies that fall under the term 'Internet service provider' of Section 702 of FISA, since the EU's Court argued that these actors could only use other data transfer tools (such as Standard Contractual Clauses) if they adopt 'supplementary measures' to protect the data from US surveillance authorities. Unfortunately, so far, there has been no identified technology that could provide the necessary additional protection besides cumbersome solutions such as 'bring-your-own-key' (BYOK) encryption for Cloud. Most industry stakeholders hope that the new framework will provide an effective and robust solution to this ongoing predicament.

Good to know: The new EU-US agreement is once again expected to be challenged by digital rights activists on the grounds that the US has not introduced meaningful (legal) safeguards since the invalidation. Infamous activist Max Schrems and his association NOYB ('None of your Business') are already sharpening their knives to bring the case back to the EU Court, which could lead to another invalidation ('Schrems III'). However, NOYB noted that in this case, they might also request the Court to suspend the application of the mechanism until the Court makes a judgment, in order to remove the incentive of adopting a non-compliant regime just to buy a few years while the Court is deliberating the case. Should this succeed, EU-US data transfers could remain a legal landmine for several years to come.

ePrivacy Regulation

■ Ongoing legislative procedure ■ Regulation 🔗 Legislative text

What is it: This legislation is an update to the ePrivacy Directive (ePD), famous for regulating access to on-device data by companies (which is why it is also known as the EU's 'cookie law'). It was originally intended to enter into force at the same time as the GDPR (2018), but has suffered multiple setbacks. Although not quite deadlocked yet, the file continues to proceed very slowly.

Where do we stand: Although already in its final stages, the procedure is not expected to be finalized before 2023. It would apply from around 18 months afterward.

Next steps		
Final agreement	*Entry into force*	*Entry into application*
Q1-Q2 2023	Q2-Q3 2023	2024-2025

Relevance for i2C:

- Cookies for EU users: many hope that the ePrivacy Regulation will provide a solution to the 'cookie banner fatigue' that was caused by the Directive's requirement for specific consent for cookies when visiting a website. However, it is unlikely that the Regulation will lead to an easing of requirements - instead, it is expected that it will establish technical ways for users to accept or reject cookies within the browser.
- Data retention: The ePrivacy Regulation is the main legal basis for Member States' Data Retention laws. Although a largely contentious point, the Regulation could introduce additional obligations to telcos and infrastructure service providers regarding retaining (meta)data about their users' activities.

Good to know: In 2014, the European Court of Justice decided that EU law does not allow for the imposition of blanket obligation on telcos to retain user data and therefore invalidated the EU Data Retention Directive, which contained obligations to this end. Member States tried to argue that EU law does not apply in this field since it concerns national security, which is exempted from EU law, but the Court held that this applies only to the direct activities of authorities but not to data collected by private actors, later to be used by these authorities. Therefore, in this revision of the ePD, Member States are trying to explicitly exempt private companies' activities related to national security from the scope, which would allow them to oblige telcos and other service providers (including potentially also infrastructure providers) to retail (meta)data of all their users. The Parliament's negotiating team, led by unyielding digital rights champion Brigit Sippel, strongly opposes these attempts.

EU-US Trade and Technology Council (TTC)

■ Ongoing non-legislative procedure 🔗 EU Communication 🔗 TTC Futurium website

What is it: The TTC aims to foster cooperation on trade and technology-related issues.
This group was created in June 2021 in which there are ten different working groups that come together to translate political decisions into deliverables, coordinate and report to the political level.

Overview of working groups:

Working Groups	
Technology Standards	Misuse of Technology Threatening Security & Human Rights
Climate and Clean Tech	Cooperation on Export Controls of Dual-Use Items
Secure Supply Chains	Investment Screening Cooperation
ICTS Security and Competitiveness	Promoting SME Access to and use digital technologies
Data Governance and Technology Platforms	Global Trade Challenges

Next steps	
Next meeting	*What to expect?*
December 2022 or January 2023 in either Austin or Miami.	Among others, Standards (e.g. electric charging, artificial intelligence), telecom infrastructure (incl. in emerging economies)

Relevance for i2C:

- A large number of topics. The most recent TTC meeting was in Paris in May 2022, in which discussions focused on, among other things, Technology Standards of AI, platform governance, SMEs access to technology, climate aspects of trade and technology, trade barriers and IoT. Generally most of the topics discussed are directly related to business activities of i2C members.

Good to know: On the EU - US TTC Futurium website, the latest publications of all working groups can be found publicly after creating an account.

Law enforcement

Terrorist Content Regulation

■ In force ■ Regulation 🔗 Legislative text

What is it: This Regulation aims to limit the dissemination of terrorist content online through prevention, detection, and removal of illegal content, including hatred, violence and terrorist propaganda.

Where do we stand: Four years after the Commission's initial publication, the Regulation has been fully applicable since June this year.

Previous steps		
EP Plenary adoption	*Entry into force*	*Compliance*
April 2021	6 June 2021	7 June 2022

Relevance for i2C:

- Terrorist content must be removed within one hour: hosting services providers (HSPs) regardless of their place of establishment or their size should remove terrorist content one hour after receiving an order from national competent authorities.
- Proactive measures and complaint mechanism: HSP will have to take proactive measures to protect their platforms and their users from terrorist abuse as well as put in place a complaint mechanism.

Good to know:

- Member States will have to put in place financial penalties for non-compliance with removal orders up to 4% of worldwide turnover.
- The one-hour rule has been widely criticized by stakeholders, particularly for smaller companies, without success.

e-Evidence package

■ Ongoing legislative procedure ■ Regulation 🔗 Legislative text

What is it: e-Evidence will allow EU MS law enforcement authorities to request information regarding ongoing criminal cases directly from i2C members. Authorities are to prioritize contacting the owner of the information directly (e.g. a website or chat service), but they will also be able to send their requests to infrastructure providers (e.g. if the former would jeopardize the investigation). The data requested could range from IP addresses to the content of communications.

Where do we stand: This procedure is in its final stages, and an agreement is expected to be found before the end of the year.

Next steps		
Official publication	*Application date*	*Deadline for designating a legal representative*
Q4 2022 / Q1 2023	Q3-Q4 2024	Q1-Q2 2025

Relevance for i2C:

- Short deadlines**:** The Regulation will allow judicial authorities in one Member State to request electronic evidence (e.g. e-mails, messages, online activity) to be provided directly from a service provider, and to receive them within a specific timeframe. This is normally 10 days but can be as low as 8 hours in emergency cases (e.g. if there is an imminent life threat).
- Legal representatives**:** When a service provider does not have its main establishment in the EU, it will be obliged to designate a legal representative for receiving and complying with EPOC / EPOC-PR. The service provider and its legal representative will be jointly and severally liable for any non-compliance.
- Sanctions for non-compliance**:** Member States will be able to impose pecuniary sanctions for infringements by service providers of up to 2% of total worldwide annual turnover.
- Reimbursement of costs**:** Positively, it is expected that service providers will be able to claim reimbursement of their costs incurred by providing e-Evidence to authorities.

Good to know: The main controversy around this file is related to fundamental rights. Left-leaning groups expressed their concern that this legislation could be (ab)used by certain countries with rule of law issues (e.g. Hungary, Poland) to restrict fundamental rights such as freedom of expression by prosecuting journalists. As such, we expect that according to the final agreement, there will be a ‘check’ by the authority of the Member State of the service provider to ensure that the request complies with fundamental rights and principles. However, this check will not apply if an authority requests data from a foreign company about a person living on the former’s territory since this is viewed by Member States as a purely internal matter (‘residence criterion’).

EU-US law enforcement cooperation

■ Ongoing non-legislative procedure 🔗 EU Communication

What is it: This cooperation is an "umbrella agreement" between the US and the EU aiming to facilitate the exchange of personal information for the purpose of prevention, detection, investigation, and prosecution of criminal offenses, including terrorism.

Where do we stand: Before the procedure could start, the EU must agree on its own e-Evidence rules. However, negotiations could start in early 2023, although due to their complexity and sensitivity, it is hard to predict how long they will take.

Next steps		
Agreement on internal rules	*Start of negotiations*	*Agreement*
Q4 2022	2023	2023-2024

Relevance for i2C:

- An accelerated process. EU countries still mostly rely on cumbersome MLAT procedures to obtain data from US companies. The new agreement could help to significantly speed up the process, which may eventually result in substantially higher amounts of requests from EU authorities for data toward i2C members.
- A limited impact. However, in many EU Member States (including Germany for example), authorities already assert (extraterritorial) jurisdiction over the activities of US companies, as long as they are available in the EU. As such, it is possible that the agreement will not make a significant difference when compared to the internal EU rules on e-Evidence. In this sense, they may even help in providing more legal certainty for service providers.

Good to know:

- The agreement has been negotiated for multiple years now, but the EU always maintained the position that it will only agree to an EU-US mechanism after it had adopted its own internal e-Evidence rules. However, now that this internal agreement is within reach, negotiations with the US can commence in earnest.
- The concerns with the agreement, raised, for example, by the EU's Data Protection Supervisor (EDPS), are similar to the e-Evidence package - the risk of misuse by Member State authorities and the need for additional safeguards. The EDPS recommended that for each request, the judicial authorities of the state in which the service provider is located in should at least be informed so that they can raise any potential concerns (e.g. if US authorities ask for data in a case where they are seeking the death penalty, or when a Member State authority could be misusing the tool to collect information on political dissidents, etc.).

Cybersecurity

NIS2 Directive - Revision

■ Finalized legislative procedure ■ Directive 🔗 Legislative text

What is it: The NIS Directive is the EU's main cybersecurity legislation. It applies to sectors considered critical for the EU, such as basic amenities (energy, water, etc.), but also to digital providers such as DNS providers, TLD registries and registrars, cloud and CDN providers, and IXPs, among others.

Where do we stand: An agreement was reached between the three institutions in May 2022 and is expected to be formally accepted by the European Parliament in September. The text will come into force 20 days after its publication and member states will have 21 months to transpose it at a national level.

Next steps		
EP Plenary Vote	*Entry into force*	*Transposition into MS national laws (21 months after OJ)*
September 2022	Q4 2022 / Q1 2023	Q2-Q3 2024

Relevance for i2C:

- Reporting obligations**:** covered entities will have to report (to the authority of their main EU establishment) any significant cybersecurity incidents with strict deadlines (a first notification within 24 hours).
- Domain name registration data: TLD registries and registrars will face stricter obligations to verify (and provide access to) registration data.
- Risk management obligations: covered entities will have to fulfill specific requirements in order to manage and mitigate their cyber risk.
- Strict supervision and enforcement**:** May include *ex-ante* elements such as on-site inspection and security audits and scans. Fines could go as high as 2% of annual global turnover, and may even lead to a ban against board-level personnel for continued non-compliance.
- Certification and standards: Member States will be empowered to oblige certain entities to use ICT products, services, and processes that were certified under EU Cybersecurity certification schemes (or, in their absence, national schemes or international standards). Moreover, the Commission will also be empowered to oblige certain categories of entities to use such EU-certified products/services and processes.

Good to know: The final text leaves room for Member States to decide how they want to 'designate' the entities that fall under the legislation. For example, authorities in different states may decide to require companies to 'self-designate' by obliging them to flag if they believe they fall under the scope of the Directive. In this case, failure to self-designate may lead to a fine at Member State level.

eIDAS Regulation - Revision

■ Ongoing legislative procedure ■ Regulation 🔗 Legislative text

What is it: The European digital identity framework aims to improve interoperability between digital identity wallets (for authentication and identification of citizens) and create a clear framework for trust service providers (TSP - digital signatures and web certificates, etc.)

Where do we stand: The first round of negotiations is almost done and both the European Parliament and Council should reach an agreement by the end of the year. Another 6-12 months will be required for Trilogue.

Next steps		
Start of trilogue negotiations	*Final agreement*	*Entry into force*
~ Q1 2023	~ Q3/4 2023	~ Q4 2023

Relevance for i2C:

- Identity verification: eIDAS simplifies the identity verification process for natural and legal persons living in the EU. Online ID verification can be useful in certain situations such as the creation of regulated TLDs or advanced website certificates that require some background check (OV/EV).
- Website certificates: The law defines new requirements for trust services providers (including website certificates).
- New fines: up to 7,000,000€ or 1,4% of the total worldwide annual turnover might be enforced in case of noncompliance for non-qualified TSP (amendment to be confirmed).

Good to know:

- The proposed law is a revision of the first one and has been well received by stakeholders and politicians.
- The Commission's target is to reach 80% use by 2030.
- Article 45-2 on a new advanced certificate for websites (QWACs) is facing a lot of criticism and was either deleted or watered down by MEPs.

Cyber Resilience Act (CRA)

■ Upcoming legislative act ■ Regulation 🔗 Call for evidence

What is it: The CRA will establish common cybersecurity standards for connected objects (IoT), including standalone software and ancillary services.

Where do we stand: This procedure hasn't started yet and the Commission should publish the text in early September. It will then require around 12-24 months to finalize and another 6-24 months to enter into application.

Next steps			
Commission's publication	*Start of negotiations*	*Start of trilogue negotiations*	*Final agreement*
13 September 2022	~Q4 2022	~Q3/4 2023	2024

Relevance for i2C:

- Keeping our eyes open: It is still too early to determine with certainty the possible links with i2C as the text is not published yet and the scope not clearly defined. However, as the supply chain is mentioned, we can expect a few surprises at the time of publication. We will keep you posted in the next newsletter.

Good to know: A first call for evidence was published by the Commission in March 2022 and received about one hundred contributions. Stakeholders are welcoming this regulation as IoT is often seen as a weak link.

Cloud Cybersecurity Certification Scheme (EUSC)

■ Ongoing non-legislative procedure 🔗 ENISA / First draft

What is it: A certification scheme to create European-wide standards for cloud security for cloud providers and services. It is not mandatory yet, but there are signs that its use could gradually become so, especially for more sensitive uses (e.g. cloud services for healthcare purposes).

Where do we stand: The scheme has been drafted already, but it has been delayed due to controversies regarding some aspects relating to 'digital sovereignty'. Once finalized, the scheme will be adopted via secondary legislation which will take around 4-6 months, after which companies will be able to certify their services via the scheme.

Next steps		
Negotiation among Member States	*Adoption*	*Entry into force 2 years after adoption*
Q3 2022	End of 2022	End - 2024

Relevance for i2C:

- Sovereignty/localization requirements: In the latest documents there were references to sovereignty, implying that only entities that have structured cooperation with a European cloud service provider could qualify for certification.

Good to know: The European Cybersecurity Agency (ENISA), through the Cybersecurity Act, is in charge of supervising, promoting, and evaluating the process of certification and standardization in order to ensure a good level of safety across the Union.

DNS4EU

■ Study / Tender 🔗 Call for tender

What is it: The EU has launched an €80 million call for tender to create its own secure and privacy-friendly DNS resolver for EU-based users as an effort to improve its cybersecurity and resilience.

Where do we stand:

Next steps		
Deadline for tender	*Next steps are not public yet*	-
20 April 2022	TBC	-

Relevance for i2C:

- DNS4EU is a direct alternative to large commercial DNS such as Cloudflare and Google.
- As DNS4EU aims to implement content filtering in its core, this might spark again the debate on the responsibility of DNS resolvers.

Good to know:

- The EU will sponsor the tender winner for a period of three years.
- DNS4EU will work closely with EU and member states' computer emergency response teams (CERT) to perform content filtering.
- The RIPE NCC (regional Internet registry for Europe) community showed perplexities about the EU initiative and wondered whether this project is useful or necessary.