

CHAIRE VP-IP

**VALEURS ET POLITIQUES
DES INFORMATIONS PERSONNELLES**

DONNÉES, IDENTITÉS ET CONFIANCE À L'ÈRE NUMÉRIQUE



Institut Mines-Télécoms Brussels Office

Values and Policies of Personal Information Research Chair

Publication Directors - Ivan MESEGUER, Claire LEVALLOIS-BARTH

Editor - Ninon BOUDES

Newsletter n°25 – July 2025



Newsletter n°25 - July 2025

Axis 1 – Digital identities	3
Digital identities at the heart of the European executive's digital strategy.....	3
Axis 2 – Privacy as a business model	4
The GDPR in a few figures: the economic impact of data protection.....	5
News brief.....	6
Axis 3 – Data sovereignties	8
News brief.....	8
Axis 4 – Intelligences and world of data	10
The implementation of the AI regulation raises questions.....	10
News brief.....	11
TO KNOW/ TO READ	12
EUROPEAN PUBLIC CONSULTATIONS.....	14
AGENDA	15



Axis 1 – Digital identities

Digital identities at the heart of the European executive's digital strategy

Designated as “core priorities for cooperation with partner countries” alongside cybersecurity and emerging technologies (artificial intelligence, 5G/6G, quantum and semiconductors), digital identities and Europe's public digital infrastructure are at the heart of the [International Digital Strategy for Europe, published on June 5, 2025](#). The European Commission shares its ambition to extend its partnerships with third countries in order to progress towards mutual recognition of electronic signatures and other trust services. In particular, this involves developing a set of tools and services for global recognition of trust services and digital identities, and thus eliminating digital barriers by reusing and [replicating the infrastructure of European electronic trust services](#) on their territory. To this end, the European Union will be collaborating with Ukraine, Moldavia, the Western Balkans, Egypt, India, Brazil, Uruguay, Japan and members of the Central American Integration System.

Over the period 2025-2027, the EU also intends to promote cooperation on public digital infrastructures by supporting the creation of a scalable suite of open-source digital solutions for digital identity wallets. In addition, the European executive will focus on demonstrating interoperability between the European digital identity wallet and similar initiatives in third countries (such as Japan, India or Singapore) on the basis of use cases (e.g. the exchange of electronic attributes and credentials in areas of common interest such as transport, travel, healthcare or academia). The European e-invoicing model will also be the focus of international cooperation.

Alongside Japan, Canada and India, the European Commission wants to standardize digital identity solutions. To this end, it intends to build on the [Architecture and Reference Framework \(ARF\)](#) of European digital identity wallets to provide a global example of reliable, secure identification with a high level of assurance.

As part of its digital strategy, the European Commission also plans to cooperate with EU candidate countries to prepare for the integration and development of interoperable solutions for online administrative procedures and the implementation of the Once-Only Technical System¹ as part of the [Single Digital Gateway](#) for these countries. Finally, the European Union wishes to pursue its work on the creation of a standardized, interoperable framework for digital health identifiers and certifications, such as the [Global Digital Health Certification Network with the World Health Agency](#).

¹ The Once-Only Technical System is a technical solution enabling public authorities to efficiently and securely exchange credentials across borders when citizens need them.



Axis 2 – Privacy as a business model

The European Data Protection Board puts personal data transfers to third-country authorities in order

At its latest plenary session on June 5, 2025, the European Data Protection Board (EDPB) adopted [its guidelines on the application of Article 48 of Regulation \(EU\) 2016/679 regarding data transfers to third-country authorities](#).

As a reminder, [Article 48 of the General Data Protection Regulation](#) (GDPR) deals with unauthorized transfers or disclosures of personal data outside the European Union. Among other things, it prohibits data transfers based solely on foreign injunctions. In July 2020, the Court of Justice of the EU invalidated the Privacy Shield, the international agreement aimed at framing transfers of personal data from the EU to the United States, ruling that the agreement was contrary to Article 48. A new legal framework for EU-US transfers was then put in place in 2023, the EU-US Data Privacy Framework, also considered legally fragile by some players².

The Board's guidelines aim to clarify the rationale and purpose of Article 48 of the GDPR, including its interaction with the other provisions of [Chapter V of the GDPR dealing with transfers of personal data to third countries or international organizations](#). The aim here is to provide practical recommendations for EU data controllers and processors likely to receive requests for disclosure or transfer of personal data from authorities in third countries. To this end, the guidelines focus on requests for direct cooperation between a third-country authority and an EU private entity (as opposed to other scenarios where personal data is exchanged directly between EU and third-country public authorities, for example on the basis of a mutual legal assistance treaty). Such requests may come from a variety of public authorities, including those overseeing the private sector, such as banking and tax regulators, as well as law enforcement and national security authorities.

The EDPB recalls that, in all cases, a “two-step test” must be applied to any transfer of personal data to third countries: “First, there must be a legal basis for the data processing together with all relevant provisions of the GDPR; and secondly, the provisions of Chapter V must be complied with. Hence, the processing i.e., the transfer or disclosure of personal data must adhere to the general principles of Article 5 and must rely on a legal basis as stated in Article 6 GDPR.” Furthermore, any transfer to a third country must imperatively be based on one of the mechanisms provided for in Chapter V of the GDPR, namely:

- An adequacy decision taken under Article 45,

² [Case T-553/23, C/2023/348 – Action brought on 6 September 2023 – Latombe v Commission](#)

- The existence of appropriate safeguards in accordance with Article 46, such as standard contractual clauses, Binding Corporate Rules (BCR) or other recognized mechanisms,
- Failing that, the application of one of the derogations restrictively listed in Article 49 of the GDPR, under the strict conditions of their implementation.

Finally, the EDPB stresses that in the absence of a legal basis under Article 6 and a valid transfer mechanism under Chapter V, the disclosure of personal data to an authority in a third country is strictly prohibited under the provisions of the GDPR.

The publication of these guidelines could well reignite debates about the validity of the Data Privacy Framework, for which the [Board had recommended ongoing monitoring](#).

The GDPR in a few figures: the economic impact of data protection

In 2023, the CNIL³ had announced that it had set up an economic analysis mission, keen to take an attentive look at the interests of the economic world. The authority published [its analysis on June 2, 2025](#).

According the French authority, “economic theory shows that corporate self-regulation leads to insufficient investment in cybersecurity. The GDPR fills these gaps, generating economic benefits due to the security obligation. These gains can be illustrated by a case study on identity theft, which estimates that the GDPR has generated benefits between €585 million and €1.4 billion in the EU, solely through the effect of notifying data breaches to the individuals concerned. 82% of these benefits are realized by companies”.

The authority's analysis highlights the fact that companies are under-investing in data protection. Indeed, faced with the potential negative consequences in terms of reputation (in cases where companies are responsible for breaches of their customers' data), companies tend to invest less in cybersecurity. This behavior leads to an asymmetry of information, with customers having no way of knowing which company was responsible for the data breach at the root of their identity theft. Yet [Article 34 of the GDPR](#) makes it mandatory to communicate personal data breaches on pain of financial penalties.

The CNIL also notes a lack of coordination with regard to the interdependence of companies. The latter do not take into account the risk of contagion of cybercrimes on other companies, when making their cybersecurity investment decisions.

³ The *CNIL (Commission Nationale de l'Informatique et des Libertés)* or National Commission for Information Technology and Freedoms is the French supervisory authority for the protection of personal data.

In addition, the ransomware⁴ market has been identified as a further cause of underinvestment. “Individuals and companies that do not implement adequate cybersecurity measures risk being hit by ransomware, which increases the overall demand from the cybercriminal’s perspective and thus drives up ransom amounts, ultimately negatively impacting society. This externality causes underinvestment in protective measures such as data backups”. The CNIL thus estimates the underinvestment blow for companies at between 20% and 66%.

While the authority has not assessed the impact of the presence of a data protection officer or that of the introduction of cybersecurity standards (Article 32 of the GDPR), it reveals that the GDPR has prevented between 54 and 132 million euros in losses linked to the direct costs of identity theft in France, and between 405 and 988 million euros in losses on a European scale.

News brief

The United Kingdom adopts a simplified version of GDPR

On June 11, 2025, the UK Houses of Parliament passed the [Data \(Use and Access\) Bill](#). Prior to its adoption, two bills had been rejected. This final text amends certain provisions of the UK GDPR and Privacy and Electronic Communications Regulations, particularly those on access to data for scientific research, or the rules applicable to fully automated decisions.

In early June, the [international advocacy group European Digital Rights](#) had encouraged the European Commission not to rule on an adequacy of this new law, which would weaken protection guarantees. Indeed, in accordance with Article 45 of the GDPR, the European Commission must adopt an adequacy decision in order to attest to the equivalent level of protection, a decision that conditions the authorization of data transfers between the European Union and a third country. In May 2025, the [European Data Protection Board granted the European Commission a further six months to assess the level of protection once the law had been adopted](#). In addition, on June 24 the Commission had adopted a six-month extension of the two adequacy decisions (one relating to the GDPR and the other to Directive (EU) 2016/680 LED) with the United Kingdom, allowing the free flow of data with this country to continue until December 27, 2025.

Simplification of GDPR worries e-tailers

In [a letter](#) to the Commissioner for Digital Sovereignty, Henna Virkkunen, and the Commissioner for Democracy, Justice and the Rule of Law, Michael McGrath, the [European lobby Ecommerce Europe](#) has expressed its opposition to the reopening of the GDPR. The lobby warns of the risks of the regulation becoming unbalanced, fragmenting the internal market and weakening fundamental rights, although Michael McGrath has defended a proportionate and balanced approach. He also announced “an implementation dialogue” for potential further simplification measures. For its part, Ecommerce Europe is calling for the

⁴ The aim of a ransomware attack is to block access to equipment or systems, or to encrypt and/or copy data, in exchange for a ransom.

strengthening of supervisory authorities, harmonized application of the GDPR and support for SMEs and companies that have made significant investments to ensure compliance.



Axis 3 – Data sovereignties

News brief

Tech industry mixed on future digital fairness regulation

On the occasion of the European Tech Summit 2025, DG Just⁵ Head of Unit Maria-Myrto Kanellopoulou stated that the [Digital Fairness Act](#) will contribute to simplification and will not duplicate existing regulations. These words echo those of DG Connect⁶, who assured us that there would be no rush towards new legislation. As a reminder, this regulation on digital equity, scheduled for the third quarter of 2026, is awaiting the opening of public consultation and an impact study.

These interventions came just days after tech industry lobbies issued a joint statement warning of the risk of increased regulatory complexity and proposals likely to cause overlapping rules. Indeed, in early May, the [US tech lobby](#) the Computer and Communication Industry Association or CCIA and [the European Tech Alliance lobby](#) highlighted the problematic practices envisaged in the Digital Fairness Act already regulated in existing texts (e.g. AI conversational robots, online influence or targeted advertising). Nevertheless, the European Commissioner for Justice and Consumer Protection, Michael McGrath, promised in mid-May “a balanced law” examined “from the angle of competitiveness and simplification”.

Health Data Hub hosting remains in limbo after French Conseil d'Etat rejection decision

On June 25, 2025, the French [Conseil d'Etat⁷ rejected the petition](#) filed by the companies Clever Cloud and Cleyrop and a private individual, who were seeking the annulment on grounds of excess of power of an alleged decision by the Minister of Health, François Braun, having waived the adoption of a sovereign health data hosting solution within two years. The high administrative court ruled that it was impossible to rule on the Minister's renunciation, but that a temporary solution had only been proposed to the CNIL, replacing the Microsoft Azure hosting provider. According to Vincent Strubel, chief executive of the French *Agence nationale de la sécurité des systèmes d'information*⁸ or ANSSI [who appeared before the French Senate's commission of inquiry into public procurement at the end of May](#), ensuring a transition to a sovereign offering is possible, although difficult to implement for interoperability and portability

⁵ The Directorate-General for Justice and Consumers (DG JUST) *promotes social justice* by upholding the rule of law and protecting individual rights and freedoms.

⁶ The Directorate-General for Communications Networks, Content and Technology (DG Connect) *works on shaping Europe's digital present and future*.

⁷ Conseil d'État, (French: “Council of State”), *highest court in France for issues and cases involving public administration*.

⁸ ANSSI is the French Cybersecurity Agency.

reasons. In addition, the Ministerial Delegation for Digital Health has issued a [call for proposals to ensure the migration of Health Data Hub data to a new host by January 2026](#), pending the migration to a sovereign host, as provided for in the French Digital Space Act no. 2024-449 of May 21, 2024.

European start-ups raise their voices regarding the application of the Digital Markets Regulation

On June 26, 2025, a [group of European start-ups sent a letter to the European Commission](#), expressing their concerns about the potential weakening of the application of the Digital Markets Act (DMA) Regulation (EU) 2022-1925 in the context of EU-US trade negotiations. In the wake of this letter, the European Commissioner for Competition, Teresa Ribera, announced that she was considering setting up a forum for dialogue with US tech, which could enable “the existing rules to be made more flexible”. This proposal, designed to appease President Trump, nonetheless triggered strong reactions from European parliamentarians, who called on the European Commission to adopt a clear and firm stance on the matter. For some, such as MEP Alexandra Geese (Greens), relaxing competition rules in the DMA in favor of American tech would be tantamount to “declaring war on the European digital industry”. In addition, tensions surrounding this regulation are being rekindled as the sixty-day deadline for Apple and Meta to comply, following their condemnation by the European Commission in April 2025, comes to an end. While Apple seems to have made some commitments, Meta's remain to be reviewed: no immediate sanctions are to be taken by Brussels, however.



Axis 4 – Intelligences and world of data

The implementation of the AI regulation raises questions

At the Telecoms Council on June 6, 2025, the European Commissioner for Digital Sovereignty, Henna Virkkunen, said she would consider postponing the implementation of the regulation (EU) 2024/1689 on artificial intelligence. The Commissioner had already announced on June 5, 2025, during the presentation of the inter/national digital strategy, that work on the code of practice for general-purpose AI models initially expected for May 2, 2025 was still underway. To this day, it seems that the code of practice is expected to be published in July.

However, the European Commission does not rule out the possibility of using the “Stop the Clock” measure⁹, already used in Omnibus I¹⁰. This measure could well be applied within the framework of the AI Act. The idea was put forward in [a note on simplification from the Polish Presidency](#). Thus, a few months' postponement of the AI Act's application deadlines could be envisaged to ensure that the regulatory framework is fully underpinned by technical specifications. For its part, the EU AI Champions Initiative, a consortium of industrialists and tech companies ready to invest €150 billion in AI in Europe, [sent a letter to the European Commission in early July calling for a two-year postponement of the AI regulation](#).

This statement comes a month after the US administration criticized the implementation of the AI Act, pointing out [“implementation difficulties and the limits of the legislation”](#).

Pressure is thus mounting on the implementation of this AI regulation: technology associations, members of the European Parliament, NGOs and even the US administration have asked the European Commission to consider a brief pause to bring all elements of the regulation into line. Swedish Prime Minister Ulf Kristersson is also calling for a pause. In his view, the fact that [the regulation on artificial intelligence is coming into force without common standards is an example of the confusion that reigns in European regulations](#).

⁹ [Directive \(EU\) 2025/794 as regards the dates from which Member States are to apply certain corporate sustainability reporting and due diligence requirements](#) regulates this measure.

¹⁰ On February 26, 2025, the European Commission published a package of legislative proposals to simplify and lighten the administrative obligations arising from several regulatory frameworks on corporate sustainability and due diligence. Among other things, the “Stop the clock” measure postpones by two years the entry into force of sustainability reporting requirements for companies under Directive (EU) 2022/2464 on the publication of sustainability information by enterprises.

For their part, industry stakeholders have expressed concern that moving forward without finalized standards could expose companies to compliance risks.

News brief

The European Commission questions the various interactions between the Artificial Intelligence Regulation and other EU regulations

At the Digital Summit in Poland on June 18, the Commissioner for Digital Sovereignty, Henna Virkkunen, said she was aware of the existing overlaps between the AI Regulation (EU) 2024/1689 and the Digital Services Act (DSA) Regulation (EU) 2022/2065. She has announced its intention to examine “the overlapping parts and simplify them”. Issues such as the interaction between the two texts if a general-purpose artificial intelligence system is designated as a “hosting service” or major online search engine by the DSA were addressed.

In the wake of the summit, the European executive published [a document clarifying the links between AI and medical device regulations](#). Indeed, the AI regulation applies to AI medical devices, qualified as high-risk AI systems. The European Commission is thus seeking to clarify interactions with medical devices ([Regulation \(EU\) 2017/745 on medical devices](#)) and with *in vitro* devices ([Regulation \(EU\) 2017/746 on in vitro medical devices](#)).

Board of Artificial Intelligence launches consultation on classifying AI systems as high-risk

At the European Business Summit, Kilian Gross, Head of Unit at the AI Office shared his enthusiasm for making the AI Act, a compliance tool. He announced [the launch of a public consultation for the European Commission's forthcoming guidelines on high-risk AI](#). Open until July 18, 2025, this consultation focuses on the main objectives of defining classification criteria for high-risk AI systems. It should clarify overlaps with general-purpose AI rules and systems considered to present an unacceptable risk, and the obligations AI system providers must meet under the AI Act. Concrete examples and specific use cases of what the European Commission defines as “high-risk” AI should accompany the guidelines. Under the AI Regulation, the Commission must publish these guidelines covering both classification and practical application by February 2026, accompanied by illustrative lists to guide suppliers and developers.

European Commission seeks experts for AI scientific panel

Launched on June 16, 2025, [a call for expressions of interest was published](#) for the development of a scientific panel to support the AI Office and Member States in their implementation of the Artificial Intelligence Regulation. Alerting the AI Office if an AI system represents a systemic risk at EU level and advising the executive on the classification of general-purpose AI models will be among the tasks entrusted to this panel. The call for expressions of interest is open until September 14, 2025.

TO KNOW/ TO READ

RGPD

- HDPG (Greece) -18/2025, The DPA ordered the provider of DeepSeek AI to appoint a representative in the EU, according to Article 27 GDPR – ([link](#))
- TikTok sues Ireland's data protection watchdog over €530m penalty from regulator – ([link](#))

(In French, use translators)

- RGPD : TikTok écope de 530 millions d'euros d'amende, d'autres mesures pourraient suivre – ([link](#))
- La simplification du RGPD pourrait exploser en plein vol – ([link](#))
- Le CRIF dispose d'un "score" pour presque tout le monde en Autriche. Noyb a besoin de soutien pour une action collective potentielle – ([link](#))
- La base légale de l'intérêt légitime : fiche focus sur les mesures à prendre en cas de collecte des données par moissonnage (web scraping), CNIL – ([link](#))
- IA : Mobiliser la base légale de l'intérêt légitime pour développer un système d'IA – ([link](#))

FRANCE

(In French, use translators)

- La réponse de l'Etat aux cybermenaces sur les systèmes d'information civils, Cour des Comptes – ([link](#))
- Le Conseil constitutionnel censure la surveillance algorithmique des URL – ([link](#))
- La CNIL lance une consultation publique sur les pixels de tracking dans les e-mails - ([link](#))
- Bercy donnera un tour de vis souverain sur les achats des ministères en matière de cloud – ([link](#))
- Après une cyberattaque, les laboratoires Cerballiance invitent leurs clients à changer leurs mots – ([link](#))
- « Posez votre carte sur le téléphone » : l'arnaque qui peut vider votre compte en quelques minutes – ([link](#))
- L'Arcep menace Orange d'une nouvelle amende pour non-respect de ses engagements sur la fibre – ([link](#))
- Reconnaissance faciale : Darmanin veut créer un groupe de travail – ([link](#))
- Mistral va former les fonctionnaires français à l'IA – ([link](#))
- France 2030 : 3 nouveaux dispositifs lancés pour faire de la France la pionnière de l'IA et de la robotique – ([link](#))
- Le CIGREF soutient la démarche de résilience numérique portée par la France, l'Allemagne, et les Pays-Bas pour construire une Europe numérique durable et de confiance dans le cadre d'Eurostack – ([link](#))
- L'IA au service de la justice : stratégie et solutions opérationnelles – ([link](#))
- France 2030 : 11 nouveaux lauréats de l'appel à projets ECONUM pour un numérique plus écoresponsable et lancement du programme de recherche « Numérique Ecoresponsable » - ([link](#))

- ANSSI : Les essentiels du modèle Zéro Trust – ([link](#))
- PANAME : un partenariat pour l'audit de la confidentialité des modèles d'IA – ([link](#))
- RESEAUX DU FUTUR : L'intelligence artificielle et les réseaux télécom, ARCEP – ([link](#))
- En France, le recours aux logiciels espion par les services a « bondi » de +136% en 5 ans – ([link](#))
- Il génère des plaidoiries par IA, et en recense 160 ayant « halluciné » depuis 2023 – ([link](#))
- Stratégie intelligence artificielle et données de santé – ([link](#))
- Encadrement de la publicité politique ciblée : la CNIL met à jour sa doctrine – ([link](#))
- L'Etat de l'internet en France, ARCEP – ([link](#))
- Fiabiliser la vérification d'identité à distance avec l'European Digital Identity Wallet – ([link](#))

EUROPE

- Commission calls on Bulgaria to comply with the Digital Services Act – ([link](#))
- Commission calls on 19 Member States to fully transpose the NIS2 Directive – ([link](#))
- DPC statement on Meta AI - Data Protection Commission Ireland – ([link](#))
- Microsoft's vast advertising business is target of ICCL Enforce application for class action launch under EU data law – ([link](#))
- 2025 State of the Digital Decade Package – ([link](#))
- Commission accepts commitments offered by AliExpress under the Digital Services Act and takes further action on illegal products – ([link](#))
- Commission eyes ditching Microsoft Azure for France's OVHcloud over digital sovereignty fears – ([link](#))
- Data protection: Council and European Parliament reach deal to make cross-border GDPR enforcement work better for citizens – ([link](#))
- Bumble's AI icebreakers are mainly breaking EU law, NOYB – ([link](#))
- Overwhelming response as 76 respondents express interest in the European AI Gigafactories initiative – ([link](#))

(In French, use translators)

- Cloud : notre dépendance aux USA coûte « plusieurs centaines de milliards d'euros par an » - ([link](#))
- Canal + demande à la CJUE de clarifier les règles de partages des données personnelles avec des tiers – ([link](#))
- Feu vert de l'Union européenne : la Bulgarie rejoint la zone euro la 1er janvier 2026 – ([link](#))
- La Commission européenne lance des procédures contre Pornhub, Stripchat, XNXX et Xvideos – ([link](#))
- L'avocate générale Kokott propose à la Cour, dans l'affaire Google Android, de rejeter le pourvoi formé par Google et de confirmer ainsi l'amende de 4,124 milliards d'euros prononcée par le Tribunal – ([link](#))

INTERNATIONAL

- Apple Store: Epic Win – ([link](#))
- NSO Group fined \$167M for spyware attacks on 1.4000 Whatapps users – ([link](#))

- Joint Statement of the third meeting of the European Union -Japan Digital Partnership Council – ([link](#))
- UK inches towards digital ID clarity with passage of Data (Use and Access) Bill – ([link](#))
- Namibia to roll out digital ID card in July 2026 – ([link](#))
- U.S. House bans Whatsapps on official devices over security and data protection issues – ([link](#))
- Why are hundreds of data brokers not registering with States?– ([link](#))

(In French, use translators)

- Au Texas, Google accepte de payer 1.4 milliard de dollars pour violation de la vie privée – ([link](#))
- Tensions entre OpenAI et Microsoft sur fond d'accusation d'abus de position dominante – ([link](#))
- Etats-Unis : la justice veut forcer Google à vendre des technologies publicitaires – ([link](#))
- Meta veut maîtriser toute la chaine publicitaire en remplaçant les créateurs par de l'IA – ([link](#))
- Palentir s'étend dans les agences états-uniennes au risque de fusion des données – ([link](#))
- Microsoft nie avoir coupé l'accès de ses services à la Cour pénale internationale – ([link](#))
- Le Canada annule la taxe sur les services numériques pour faire progresser les négociations commerciales plus larges avec les Etats-Unis – ([link](#))

EUROPEAN PUBLIC CONSULTATIONS

Closed :

- Apply AI Strategy – strengthen AI Continent, 9 April – 4 June 2025 ([link](#))
- Cloud and AI Development Act, 9 April 2025 - 4 June 2025 ([link](#))
- A European Strategy for AI in science – paving the way for a European AI research council, 10 April 2025 – 5 June 2025 ([link](#))
- Guidelines 02/2025 on processing of personal data through blockchain technologies, 14 April 2025 – 9 June 2025 ([link](#))
- European Business Wallet, 15 May 2025 – 12 June 2025 ([link](#))
- Commission Guidelines to clarify the scope of the General-purpose AI rules in the AI Act, 22 April - 22 May 2025 ([link](#))
- Guidelines 02/2025 on processing of personal data through blockchain technologies, 14 April – 9 June 2025 ([link](#))
- European Cybersecurity Act, 11 April 2025 – 20 June 2025 ([link](#))
- Digital Network Act, 06 June 2025 - 11 July 2025 – ([lien](#))

Pending:

- European Data Union Strategy, 23 May 2025- 18 July 2025 – ([link](#))
- eIDAS Regulation – accreditation of conformity assessment bodies,– ([link](#))
- eIDAS Regulation – trusted lists, 20 June 2025- 18 July 2025 – ([link](#))
- eIDAS Regulation – risk management procedures for non-qualified trust service providers, 20 June 2025- 18 July 2025 – ([link](#))
- Omnibus Directive Aligning product legislation with the digital age, 23 May 2025 - 26 August 2025 – ([link](#))

- Consultation on the first review of the Digital Markets Act, 3 July 2025 – 24 September 2025 - ([link](#))

AGENDA

European Commission:

- July 1, 2025 - Start of the Danish Presidency of the Council of the European Union
- July 3, 2025 - Publication of code of practice on general-purpose AIs
- July 4, 2025 - EU-Moldova Summit
- July 14, 2025 - Presentation of the European Commission's guidelines on the protection of minors, as part of the implementation of the Digital Services Regulation
- Mid-July - Presentation of the post-2027 Multiannual Financial Framework, European Commission
- July 15, 2025 - Dialogue on the simplification of consumer law, European Commission
- July 16, 2025 - Second implementation dialogue on simplification on “GDPR enforcement”
- December 16, 2025 - Telecom market reform (Digital Network Act)
- December 21, 2025 - Evaluation of the telecommunications code

European Artificial Intelligence Committee:

- July 7, 2025 - Meeting of the Steering Committee of general-purpose AI providers
- July 30 - August 13, 2025 - Period of adoption of a written version of the suitability assessment of the code of practice by the high-level group