At-a-glance:
A guide to the EU's digital package

November 2025

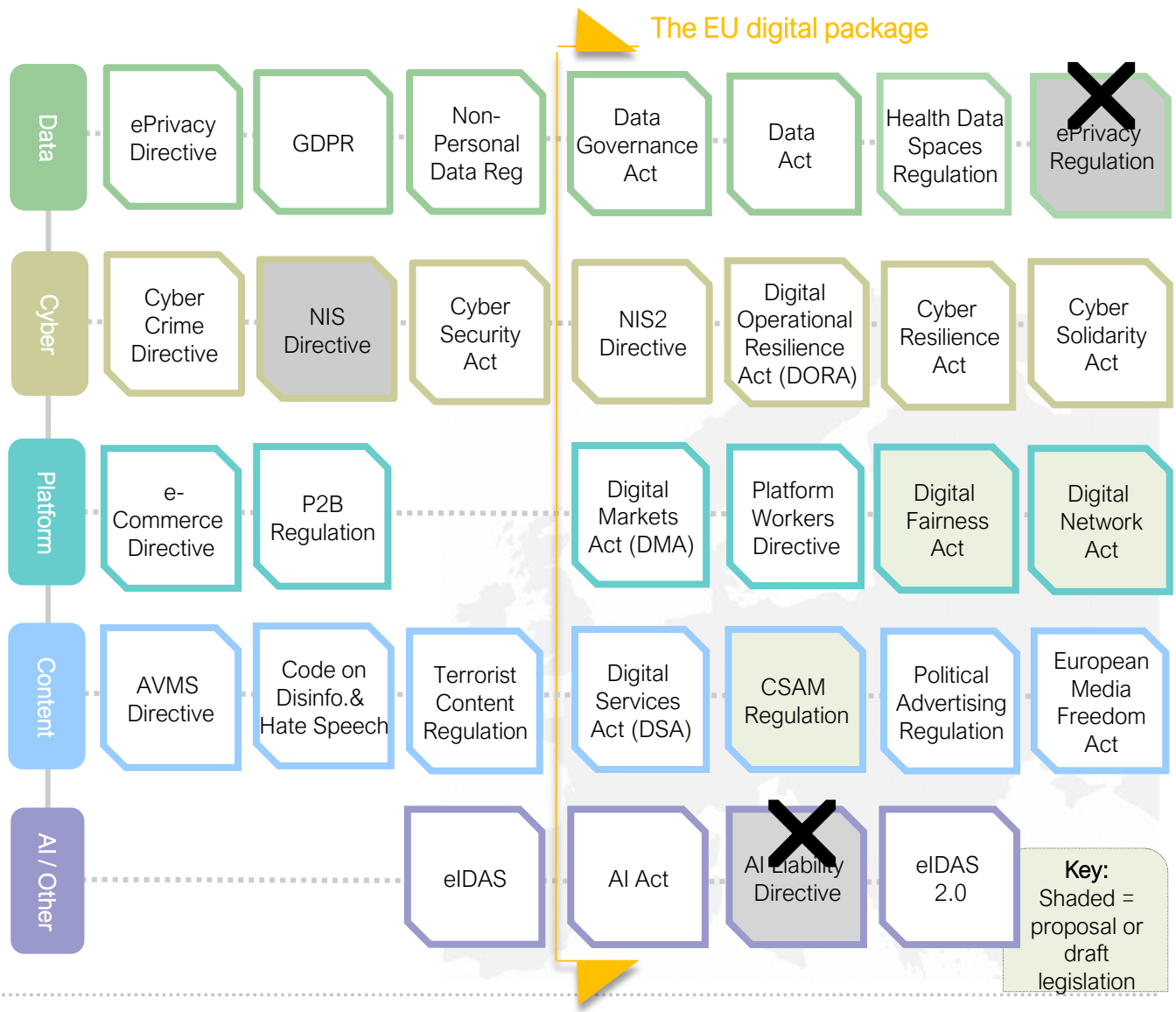
At a glance

This handbook provides an "at a glance" summary of the status of the instruments making up the EU digital package. It does not attempt to provide a detailed overview of these instruments but instead provides a high-level summary of whom they apply to, what the key obligations are and when they are likely to come into force.

The summaries are based on the text at either the proposal or adoption stage and **do not generally highlight amendments made in intermediate drafts**. This handbook is not a substitute for reading the actual instruments themselves.

This handbook also only focuses on data, cyber, platform and AI aspects of this new package. It does not include other measures to regulate crypto-currencies, tax digital activities or reform consumer protection laws.

The handbook sets out the position as at 25 November, including the proposed Digital Omnibus discuss overleaf, though the intention is to update it periodically as the digital package progresses.



The Digital Omnibus update

In November 2025, the EU Commission issued the Digital Omnibus (2025/0360 (COD)) and the Digital Omnibus on AI (2025/0359 (COD)). These proposals will make a number of significant changes to the Digital Package. Some of the key changes include:

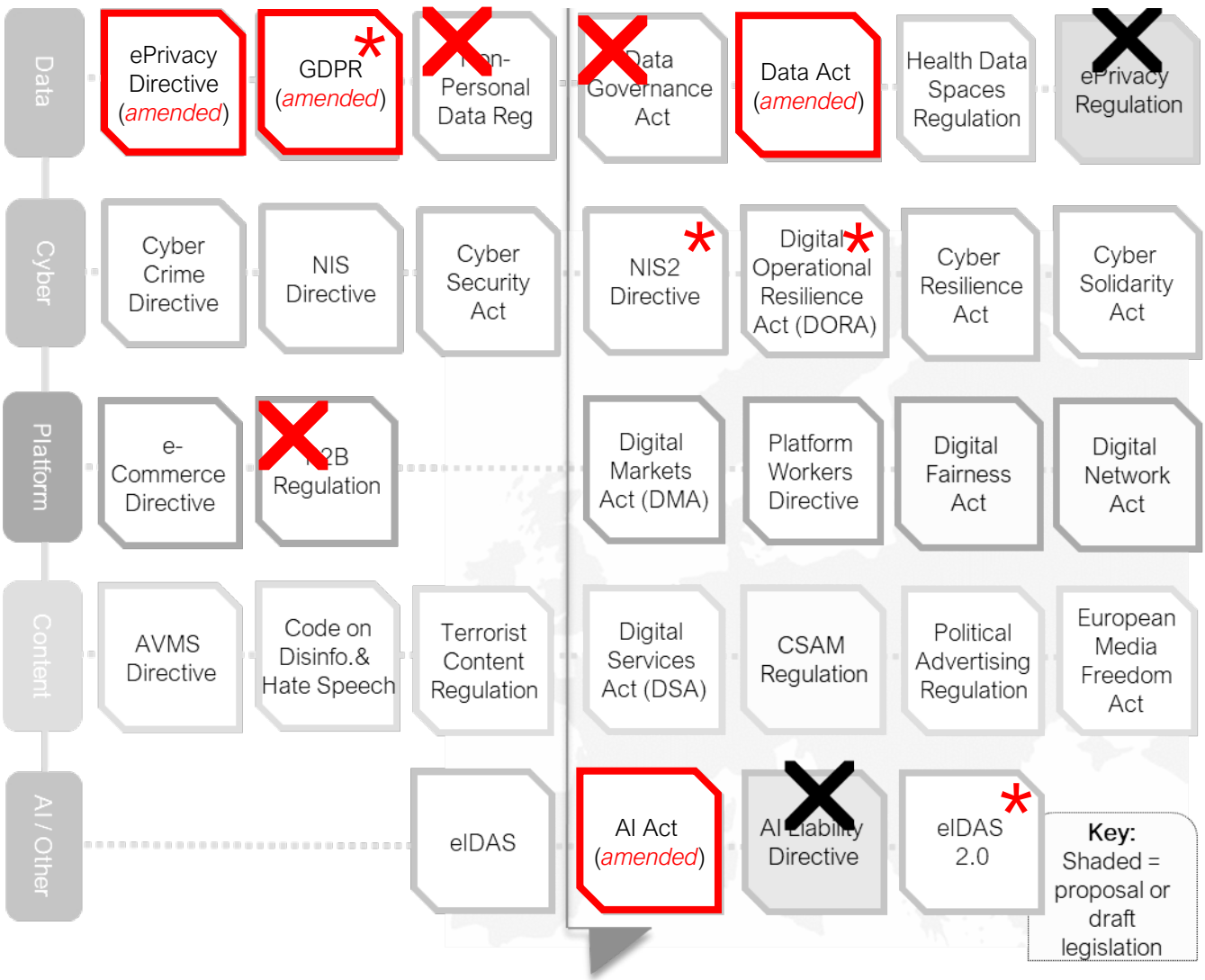
> **AI**: The AI literacy obligation will be removed. The deadline for "high risk" AI systems will be pushed back to Dec 2027 (or Aug 2028 for Annex I systems). The GDPR will be amended to permit the training of AI on personal data (inc. special category data) subject to safeguards.

> **GDPR**: There are numerous changes, including codifying the *SRB* judgment on the meaning of personal data, restricting abusive subject access requests, extending the time to notify breaches to 96 hours and relaxing the obligation to provide privacy notices for "BAU" activities.

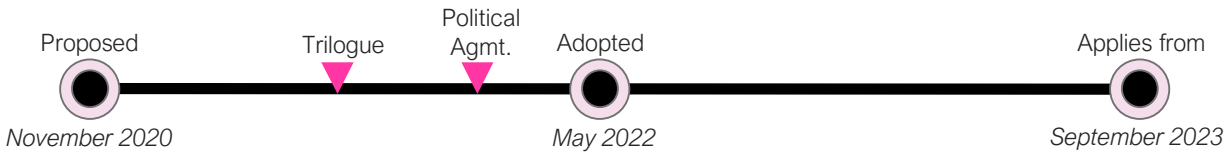
> **ePrivacy**: The cookie rules (for personal data only) will move into the GDPR with amendments to hopefully remove cookie banners.

> **Data breach**: A single-entry point will be created for security breach notifications under the GDPR, NIS2, eIDAS2, DORA and the Critical Entities Resilience Directive.

> **Data**: The Non-Personal Data Regulation, P2B Regulation and Data Governance Act will be repealed. Parts of those instruments will be added to the Data Act. There will be some relaxation of the cloud switching rules.



The Data Governance Act (Regulation (EU) 2022/868)



Summary

This EU Regulation encourages public bodies to share data, creates a regulatory framework for data intermediaries and encourages data altruism.

Who does it apply to?

The Regulation is primarily applicable to

> Public sector bodies

> Data intermediaries. These are entities that aim to create commercial relationships between (a) individuals and data holders, and (b) data users

> Data altruism organisations

Key obligations

Reuse of public information

> The existing rules on reuse of public data contain carve-outs for sensitive data (e.g. data protected by IP or containing personal data)

> The Regulation is intended to encourage public bodies to make this more sensitive data available by using protective measures

Data intermediaries

> Data intermediaries will become subject to strict new obligations, including notifying new regulatory bodies

Data altruism

> Data subjects will be encouraged to share data for altruistic purposes, e.g. health care or combatting climate change

> Data altruism organisations will be strictly regulated and subject to obligations to notify new regulatory bodies

Business impact

This Regulation should have a limited impact on most businesses

Green

Further reading

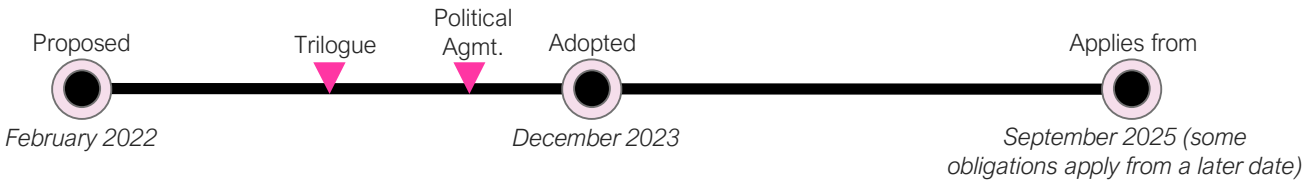
> Regulation 2022/868 on European data governance (Data Governance Act) (here)

> *New EU Data Governance Act published*, June 2022

Digital Omnibus proposal

To be repealed.

The Data Act (Regulation (EU) 2023/2854)



Summary

This Regulation will regulate the use of data from "Internet of Things" (IoT) devices and make it easier to switch between cloud services

Who does it apply to?

The Regulation is primarily applicable to

> Providers of IoT devices

> Third parties wanting to access IoT data

> Providers and users of cloud services

> Those licensing data on standard form terms

Key obligations

IoT

> Providers of IoT devices will need to make IoT data available to users

> There are complex provisions for licensing IoT data to third parties

> IoT data will not be subject to database rights

Cloud switching

> Cloud providers will be subject to a range of obligations to assist their customers to switch providers

> This includes new provisions that must be included in cloud contracts and controls on charges for switching services

> There are restrictions on cloud providers providing unlawful access to non-personal data to third-country governments

There are also provisions relating to:

> Unfair terms in standard form B2B data licences

> The provision of data to public authorities

Business impact

The provisions on access to IoT data will be important to providers of these devices

Amber

Further reading

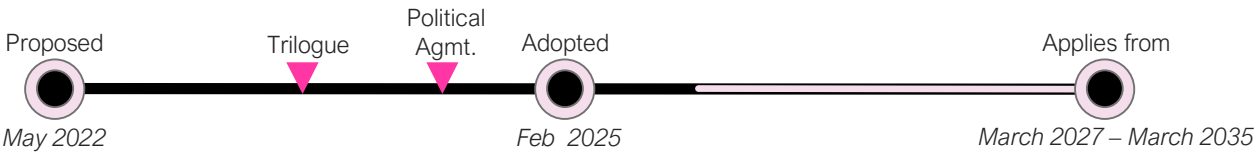
> Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act) (here)

> *The "Data Act"*, January 2024

Digital Omnibus proposal

Major amendments proposed including transferring provisions in the DGA and Non-Personal Data Regulation into the Data Act. Minor changes to cloud switching and trade secrets for IoT data.

European Health Data Spaces Regulation (Reg. (EU) 2025/327)



Summary

This Regulation will result in more health data being recorded electronically and will create a framework to allow that data to be used for secondary purposes such as research

Who does it apply to?

The Regulation is primarily applicable to

> Healthcare providers

> Researchers wanting to access health data

> Providers of electronic healthcare records (EHR)

> Providers of "wellness applications"

Key obligations

Digital healthcare records

> Individuals will have a right to immediate access to their healthcare data (including portability)

> Healthcare providers will have a right to access to EHRs to provide care

> Healthcare providers will need to record health care information into EHRs

Research and secondary uses

> A framework will be set up to allow researchers to gain access to healthcare data

> Access will be subject to approval from a "health data access body" and access to the data will be via a Secure Processing Environment

EHR providers will become subject to various duties, including compliance with a common specification and CE marking

Providers of wellness applications will be subject to labelling and registration obligations

Business impact

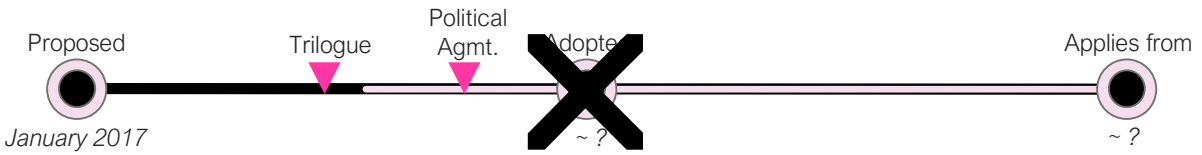
This provisions will be important to entities in the healthcare and research sectors

Amber

Further reading

> Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space (here)

ePrivacy Regulation (*Withdrawn*)



Summary

This EU Regulation will replace the existing ePrivacy Directive. However, it has had a difficult legislative passage and has now been withdrawn

Who does it apply to?

The Regulation is primarily applicable to

> All entities using electronic direct marketing (e.g. email or telephone)

> All entities using cookies

> Telecoms and messaging providers in relation to the interception of communications, use of metadata and telecoms related privacy issues (e.g. calling line identification)

Key obligations

Electronic direct marketing

> It is not clear if there will be significant changes to the current rules

> Member States might be allowed to set a maximum time limit during which such marketing can be conducted

Cookies

> There might be some minor changes such as allowing analytics cookies without consent

> The rules might address related issues like WiFi tracking and automatic software updates

Content and metadata

> There will be strict new rules on when telecoms operators and messaging providers can intercept content and use metadata

Sanctions

> Breach will result in "GDPR-like" sanctions

Business impact

The Regulation has been withdrawn

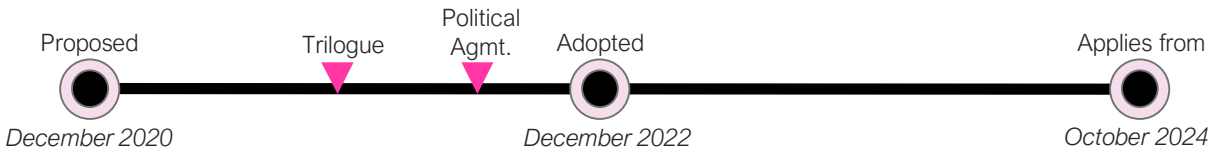
None

Further reading

> Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications (Regulation on Privacy and Electronic Communications) (here)

> *The ePrivacy Regulation - Let the trilogue begin!* February 2021

NIS 2 Directive (Directive (EU) 2022/2555)



Summary

This Directive replaces the existing Network and Information Systems Directive. It imposes cyber security and breach notification obligations on certain essential and important entities

Who does it apply to?

The Regulation is primarily applicable to

> Essential entities, e.g. those in the energy, transport, financial, health, water, digital infrastructure, ICT, public administration and space sectors

> Important entities, e.g. those in the post, waste management, chemical production, manufacturing, food production, digital and research sectors

> Member State governments who must have cyber security strategies, crisis management frameworks and incident response teams

Business impact

The Regulation arguably just strengthens existing regulation and best practice. However, direct liability of management boards is significant

Amber

Key obligations

Preventative measures

> Essential and important entities must use appropriate measures to protect their systems, including measures such as vulnerability handling and supply chain control

> Management boards must oversee these measures and are liable for a failure to comply. They must be trained in cyber security

> Member States can require certain ICT products and services to be certified

> In some cases, an EU representative must be appointed

Incident reporting

> Essential and important entities must notify significant incidents to the relevant regulatory authority, and may need to notify recipients of the service

Repeals and replaces the existing NIS Directive

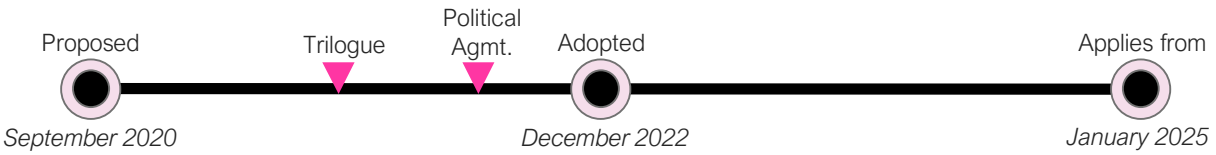
Further reading

> Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) (here)
> Three implementation issues (here)

Digital Omnibus proposal

New single-entry point for incident notifications.

DORA (Regulation (EU) 2022/2554)



Summary

The Digital Operational Resilience Act (DORA) is an EU Regulation that imposes significant cyber security obligations on financial services institutions and regulate critical third parties

Who does it apply to?

The Regulation is primarily applicable to

> Financial services institutions

> Third party service providers who provide "critical" ICT services to financial services institutions

Key obligations

Financial services institutions must apply uniform standards for managing ICT risks and to protect against cyber attacks. For example, this includes

> The management body being responsible for ICT risks

> Putting in place appropriate ICT tools and intrusion detection systems

> Conducting penetration testing

> Putting in place an incident response plan and reporting incidents to the relevant regulator

> Managing third parties according to more prescriptive rules with key contractual requirements

> Putting in place and testing appropriate resilience plans

Service providers

> Third parties which provide "critical" ICT services to the financial sector will be directly supervised

Business impact

The Regulation requires significant additional work for some financial services institutions

Red

Further reading

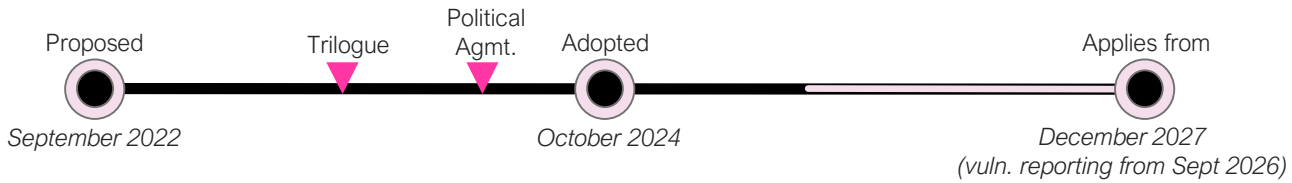
> Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (here)

> Our DORA guide (here), October 2023

Digital Omnibus proposal

New single-entry point for incident notifications.

Cyber Resilience Act (Regulation (EU) 2024/2847)



Summary

This Regulation will impose cyber security obligations on those supplying products containing digital technology

Who does it apply to?

The Regulation is primarily applicable to

> Those supplying products containing digital technology in the EU that are designed to connect to another device or network

> It does not appear to apply to "standalone" electronic devices (e.g. toasters or microwaves) unless they have IoT functionality

> However, the term "products" includes both software and hardware meaning these rules extend beyond physical goods manufacturers

Key obligations

Essential cyber security requirements

> The product shall be designed to ensure appropriate cyber security by reference to strict criteria, such as limiting attack surfaces

> A risk assessment must be undertaken

> Strict processes must be in place to identify and patch vulnerabilities

> Users must be given security information and fixed support period

> Some products will be designated as "important" (e.g. operating systems, smart home products) or "critical", and be subject to third-party conformity assessments

Vulnerability reporting

> Manufacturers must notify ENISA and national cybersecurity authorities of incidents and exploited vulnerabilities within 24 hours

Business impact

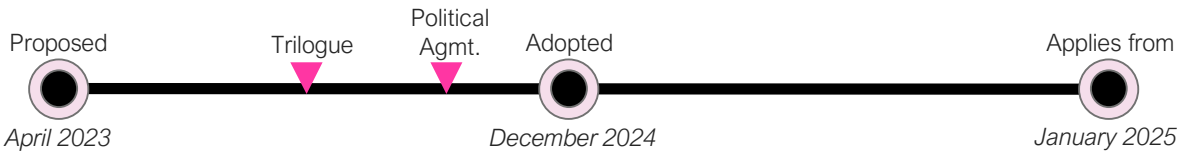
The Regulation will be a major change for those supplying digital hardware or software

Red

Further reading

> Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act) (here)

Cyber Solidarity Act (Regulation (EU) 2025/38)



Summary

The Regulation aims to strengthen solidarity in respect of the EU's detection of cybersecurity threats and improve its situational awareness, preparedness and response capabilities.

Who does it apply to?

The Regulation is primarily applicable to

> EU Member States

> European Union Agency for Cybersecurity (ENISA)

Key obligations

Creation of the *Cyber Emergency Mechanism* – This will support Member State's cyber efforts. This includes preparedness testing, which might involve private sector entities who provide critical infrastructure

Deployment the *Cyber Alert System* – A pan-European infrastructure of Cyber Hubs

Creation of the *Cybersecurity Reserve* – A pool of trusted cyber vendors who can assist Member States and EU institutions

Establishing a European *Cybersecurity Incident Review Mechanism* – This will review and assess specific significant or large-scale incidents

Business impact

The impact for most businesses is limited

Green

Further reading

> Regulation (EU) 2025/38 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents (Cyber Solidarity Act) (here)

Digital Markets Act (Regulation (EU) 2022/1925)

Summary

This Regulation imposes significant new *ex ante* obligations on 'Big Tech' gatekeepers to ensure competition in digital markets

Who does it apply to?

The Regulation is primarily applicable to

> "Gatekeepers" as 'Big Tech' providers of core platform services (including but not limited to intermediation services, search engines, social media, OS, ad services, and cloud computing)

> The Commission has designated a number of large core platform service providers as gatekeepers

> The open and fair markets focus means that the DMA is likely to be a game changer for digital markets and companies reliant on gatekeepers' services

Business impact

The Regulation is likely to have a significant effect on digital markets

Amber

Key obligations

Companies designated as gatekeepers will have to comply with a list of obligations which aim to ensure that digital markets are contestable and fair for market participants. Each obligation considers specific scenarios but the common theme is keeping digital markets "open", e.g.:

> *Restricting leveraging*: Rules limiting the gatekeepers' ability to use their core platform services to favour other services within their ecosystems, e.g. gatekeepers are prohibited from preferencing their own offers in their results rankings

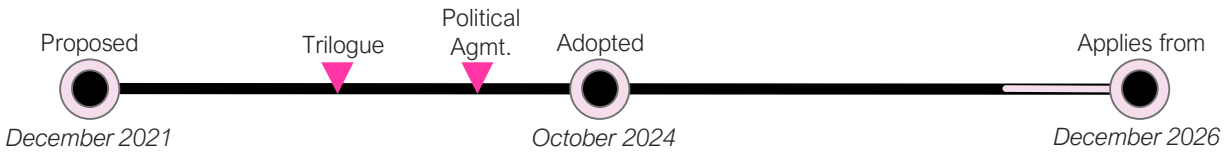
> *Paving the way for rivals*: Rules reducing barriers for challenger platforms to compete with gatekeepers, including a specific requirement to provide for messaging interoperability

> *Rebalancing power for business users*: Rules rebalancing certain aspects of gatekeepers' commercial relationships with their business users, e.g. imposing data sharing in certain circumstances

Further reading

> Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act) (here)
> Linklaters' DMA Hub

Platform Workers Directive (Directive (EU) 2024/2831)



Summary

This Directive will create a refutable presumption that those carrying out platform work will be employees and creates new rights for workers regarding algorithmic management

Who does it apply to?

The Directive is primarily applicable to

> Those providing digital labour platforms – i.e. a commercial online platform that allows customers to request services that involve the organisation of work by individuals as an essential component of that service

> This includes both solely online services (e.g. data encoding, translation, graphic design) and on-location services (e.g. ride-hailing, delivery of goods, cleaning or care services)

> These rules apply where platform work is performed by individuals in the EU, regardless of where the platform provider is based

Business impact

The Directive is likely to have a significant effect on digital labour platforms, including those located outside the EU

Amber

Key obligations

Refutable presumption of employment

> Each Member State will need to establish criteria for presuming employment, based on control and direction

Algorithmic management

> Platform workers and workers' representatives will have enhanced information rights about the use of algorithmic management

> Platform workers will have the right to human review (one-on-one conversation) and the right to contest automated decisions impacting them

> The use of some types of data (e.g. emotional state) in these systems is prohibited

Enforcement measures

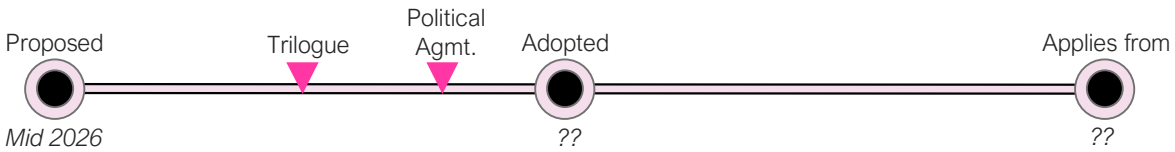
> Obligation for digital labour platforms to declare work to national authorities on a six-monthly basis

Further reading

> Directive (EU) 2024/2831 on improving working conditions in platform work (here)

> Saying goodbye to bogus self-employment and AI bosses, April 2024

Digital Fairness Act (*Awaiting draft*)



Summary

This Regulation will complement the Digital Services Act by regulating "unethical" commercial practices by online platforms. A legislative proposal is expected in mid 2026

Who does it apply to?

The Regulation will (likely) be primarily applicable to

> Online platforms, particularly VLOPs

Key obligations

The exact contents are still to be confirmed but may include:

> New concrete prohibitions of 'dark patterns'

> Mandatory 'click-to-cancel' function on platforms

> Requirements for express consent from the user when switching from free trial to paid subscription

> Restrictions on ‘harmful’ features such as loot boxes

> Restrictions on personalisation that exploits vulnerabilities, sensitive data or targets minors

> Disclosure requirements for influencers and for brands that pay for endorsements on social media

> Consumers' right to access a human interlocutor, if AI chatbots are used in customer service

Business impact

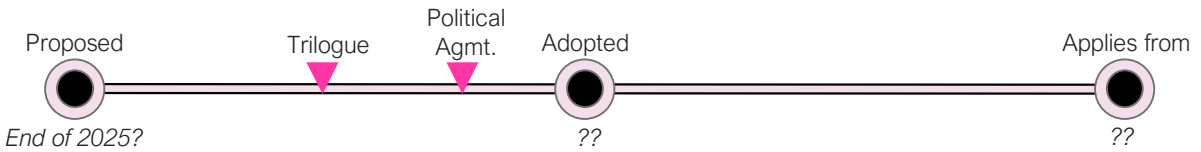
The Regulation could have important implications for online platforms

Amber

Further reading

> No further reading at this time

Digital Networks Act (*Awaiting draft*)



Summary

This Regulation will impose new obligations on telecoms companies. A proposal is expected towards the end of 2025.

Who does it apply to?

The Regulation will (likely) be primarily applicable to

> Telecoms companies

Key obligations

The exact contents are still to be confirmed but may include:

> New rules for radio spectrum management and assignment

> Rules on market consolidation among telecoms operators

> New rules on copper switch-off

> Deregulation of physical access to networks

Business impact

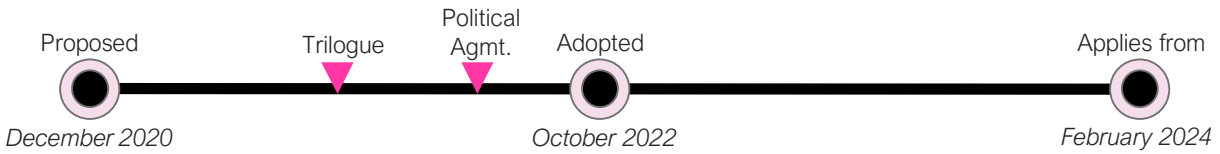
The Regulation could have important implications for telecoms companies

Amber

Further reading

> A summary of these proposals is here

Digital Services Act (Regulation (EU) 2022/2065)



Summary

This Regulation imposes new obligations on those hosting content with those providing online platforms subject to significant new "online harm" obligations

Who does it apply to?

The Regulation is primarily applicable to

> Those providing hosting, caching or mere conduit services

> Those providing online platforms, e.g. social media services and online marketplaces

> Very large ('Big Tech') providers of social media services, online marketplaces and search engines

Key obligations

Hosting, caching and mere conduit

> The intermediary defences in the old eCommerce Directive will be preserved (including a new "Good Samaritan" defence for own initiative investigations)

> However, there are new obligations such as having to appoint a single point of contact and to report annually on content removal

> Hosting providers will need to tell users when content is removed and allow them to appeal

Online platforms

> A range of significant new obligations apply such as a prohibition on "dark patterns", transparency obligations in relation to ads and recommender systems

Very large online platforms (VLOPs) and search engines (VLOSE) are subject to further obligations such as creation of an internal compliance function and conducting risk assessments

Business impact

The Regulation will be significant for those hosting content, social media, online marketplaces and search engines

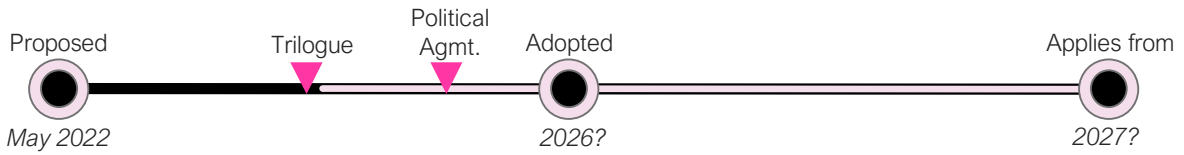
Amber

Further reading

> Regulation (EU) 2022/2065 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (here)

> *The EU Digital Services Act: A new era for online harms and intermediary liability*, February 2023

CSAM Regulation (*In draft*)



Summary

This Regulation will impose a range of obligations to remove child sexual abuse materials (CSAM), including conducting risk assessments and implementing mandatory detection orders. This has been subject to strong opposition by some Member States and is making slow progress

Who does it apply to?

The Regulation is primarily applicable to

> Hosting services

> Interpersonal communication services (messaging services)

> Apps stores

> Internet access services

Key obligations

Hosting and messaging services

> Must conduct risk assessment in relation to CSAM and take appropriate mitigation measures

> Can be subject to detection orders which require the provider to use technology to prevent the dissemination of CSAM or grooming of children

> Must report potential CSAM to the appropriate authorities

> Can be subject to a removal order (hosting services only)

App stores

> Must assess if any apps present a CSAM risk and take reasonable measures to ensure apps that present a grooming risk are not available to children

Internet access service

> Can be subject to blocking orders

Victims also have rights to information and assistance with removal of CSAM

Business impact

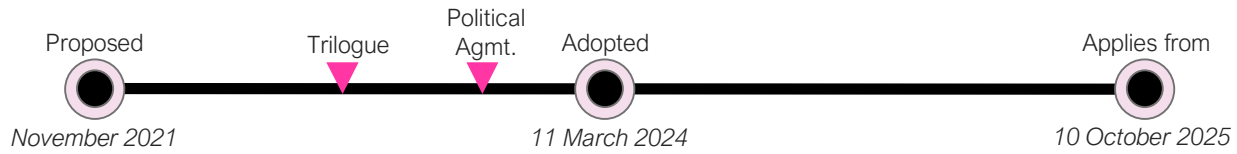
The Regulation has important implications for hosting and messaging companies

Amber

Further reading

> Proposal for a Regulation laying down rules to prevent and combat child sexual abuse (here)

Political Advertising Regulation (Regulation (EU) 2024/900)



Summary

This Regulation will require additional transparency in relation to political advertising (including targeting and amplification techniques)

Who does it apply to?

The Regulation is primarily applicable to

> Publishers of political advertisements

> Those providing political advertising services

Key obligations

Publishers

> Political advertisements must be identified as such and contain additional information such as the sponsor of the advertisement

> Where the publisher is a VLOP, this information must form part of its advertising repository under the Digital Services Act

> Remuneration or other benefits from providing political adverts must be disclosed

> User must be able to notify breach of these requirements

> Targeting and amplification based on special category personal data is prohibited (unless based on explicit consent or by a non-profit)

> Additional transparency obligations arise for targeting and amplification techniques used for political advertising and suitable policies must be developed

Business impact

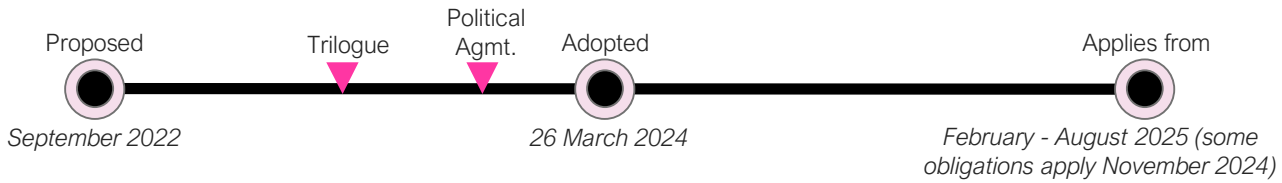
The Regulation is mainly relevant to publishers and those placing political adverts

Green

Further reading

> Regulation (EU) 2024/900 on the transparency and targeting of political advertising (here)

European Media Freedom Act (Regulation (EU) 2024/1083)



Summary

This Regulation is mainly focused on media service providers but also contains obligations for VLOPs in relation to the removal of content from media service providers and obligations for providers of media players

Who does it apply to?

The Regulation is primarily applicable to

> Very large online platforms (VLOPS) as defined in the Digital Services Act

> Providers of audiovisual media players

> Media service providers, being those that exercise editorial control over the provision of programmes or publications to the public

Key obligations

VLOPs

> Must allow media service providers to declare their status

> VLOPs are subject to transparency and consultation obligations in relation to the restriction or suspension of content from media service providers

Media services providers

> Protected against Member States: (a) interfering with editorial decisions; (b) seeking information on sources; and (c) deploying spyware

> Public media service providers are subject to impartiality obligations and controls on appointments

> Media service providers providing news must make certain disclosures and ensure editorial freedom

> Member States must assess media pluralism

Providers of audiovisual media players must allow users to customise the player by changing default settings

Business impact

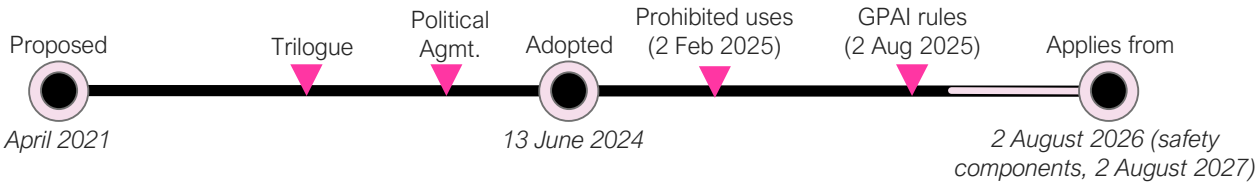
The Regulation is mainly relevant to media service providers

Green

Further reading

> Regulation (EU) 2024/1083 establishing a common framework for media services (European Media Freedom Act) (here)

AI Act (Regulation (EU) 2024/1689)



Summary

This Regulation introduces tiered regulation of artificial intelligence systems; some uses are banned, some are subject to significant compliance obligations, some are subject to very limited regulation

Who does it apply to?

The Regulation is primarily applicable to

> Those supplying or using certain types of artificial intelligence systems

Key obligations

Banned

> The use of AI for certain purposes (e.g. manipulative techniques or social scoring) is banned

High risk

> The use of AI as a safety component of certain products is "high risk"

> The use of AI for specific uses (e.g. employment assessment, education, creditworthiness) is also "high risk"

> "High risk" systems are subject to burdensome mandatory requirements and conformance assessments

General purpose AI (GPAI)

> Large GPAIs are subject to burdensome obligations. Others GPAIs are subject to more limited transparency obligations

Limited risk

> Transparency obligations apply in relation to the use of AI in human interactions

Business impact

This will be significant for those supplying or wanting to use "high risk" AIs or developing large GPAIs

Amber

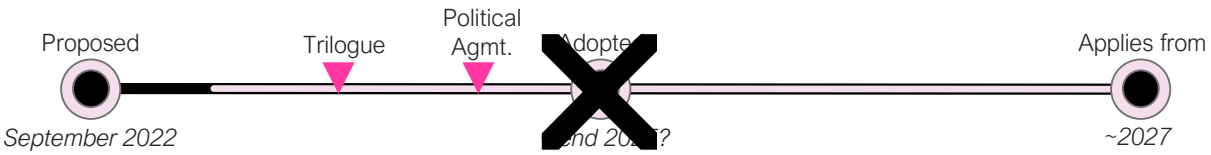
Further reading

>Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (EU AI Act) (here)
> *AI Toolkit*, July 2024

Digital Omnibus proposals

Major amendments such as the removal of AI literacy obligations. The deadline for "high risk" AI systems pushed back to Dec 2027 (or Aug 2028 for Annex I).

AI Liability Directive (*Withdrawn*)



Summary

This Directive was intended to partly harmonise rules on tortious liability for artificial intelligence systems, including disclosure obligations. It has now been withdrawn

Who does it apply to?

The Regulation is primarily applicable to

> Those supplying or using certain types of artificial intelligence systems

Key obligations

Disclosure

> Member States must implement rules to require disclosure of evidence in cases where "high risk" AI systems cause damage

Rebuttable presumption of causation

> There will be a rebuttable presumption that any fault on the part of the provider of an AI system is the cause of the output from the AI giving rise to damage

> In the case of "high risk" AI systems, fault is defined by reference to compliance with the AI Act

These rules only apply to tortious liability, e.g. non-contractual civil liability

"High risk" AI systems are those defined as high risk in the AI Act

Business impact

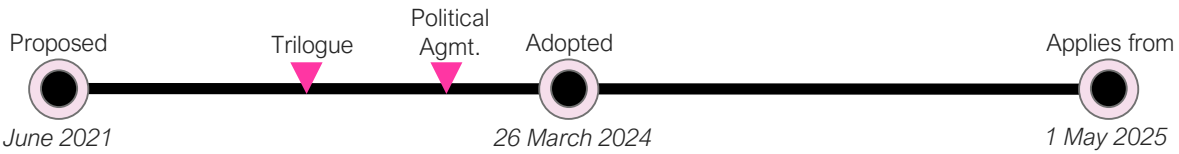
The Directive has been withdrawn

None

Further reading

> Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) (here)
> AI Toolkit

eIDAS 2.0 (Regulation (EU) 2024/1183)



Summary

This Regulation will amend the existing eIDAS Regulation to introduce Digital Identity Wallets and help with the evidential admissibility of blockchains

Who does it apply to?

The Regulation is primarily applicable to

> Those looking to authenticate individuals

> Those using blockchains

Key obligations

Digital Identity Wallets

> Member States must issue Digital Identity Wallets within 12 months of the Regulation coming into force

> The wallets allow users to store identity credentials for authentication purposes

> These wallets should allow users to electronically identify and authenticate themselves both online and offline to access public and private services

Other

> New rules on the legal effectiveness and admissibility of electronic ledgers (such as blockchains) and qualified electronic ledgers will enjoy a presumption of uniqueness and authenticity

> New rules on remote electronic signatures

> Amendments to align eIDAS with the proposed NIS 2 Directive

Business impact

The Regulation is likely to be important to those seeking to authenticate individuals electronically

Green

Further reading

> Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (here)

Digital Omnibus proposals

New single-entry point for breach notifications.

The UK approach to digital reform

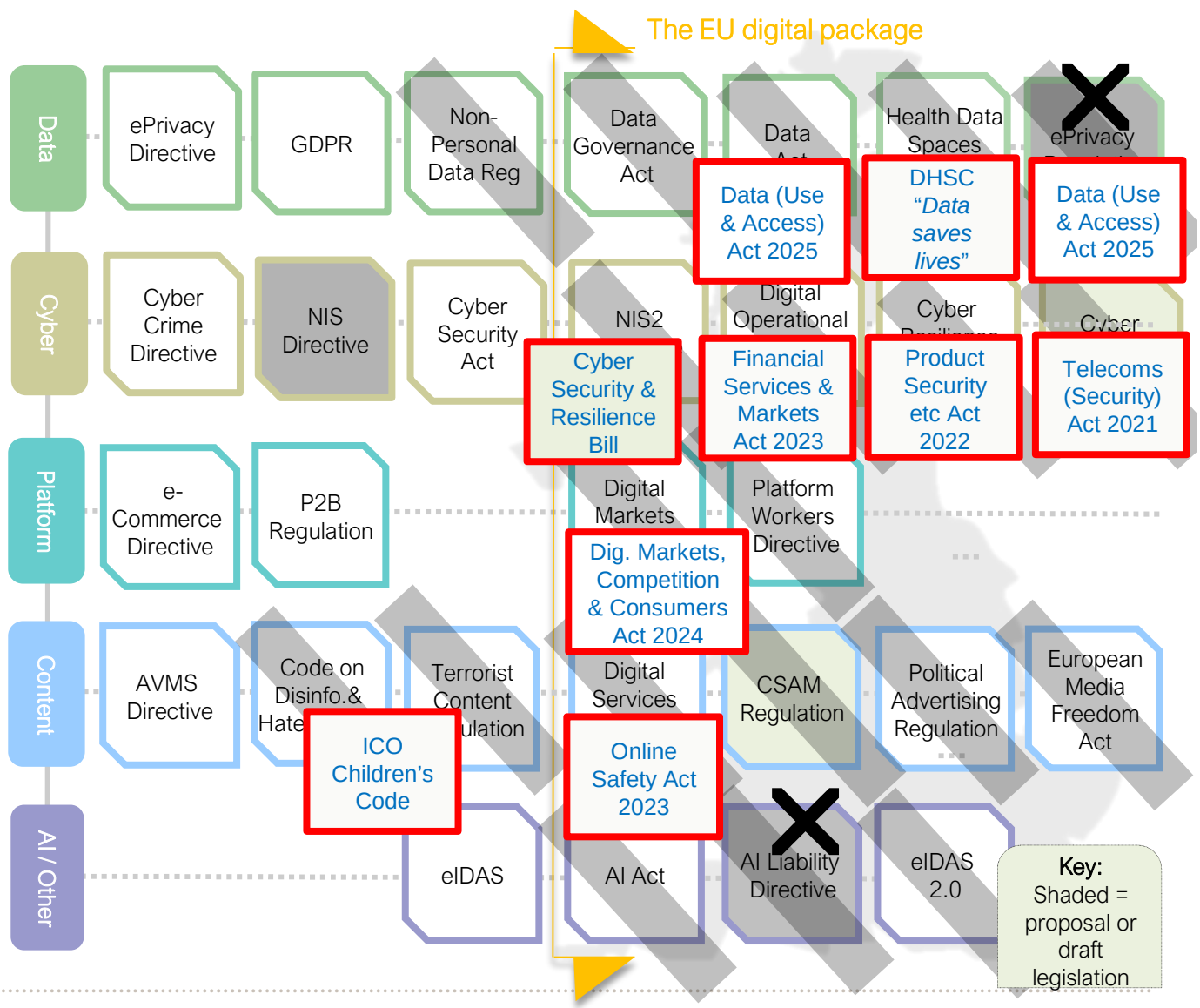
The instruments in the EU's digital package have been, or will be, adopted after Brexit and so will not become part of UK law.

However, the UK is taking a range of measures that replicate some aspects of the EU's digital package, including both legislative and policy measures. These are summarised below.

> *The Data (Use and Access) Act 2025*: This Act reforms the regulation of cookies in the UK, which was an issue addressed by the EU's now abandoned ePrivacy Regulation and the new Digital Omnibus. The Act also includes some new data rights for customers, which could replicate aspects of the EU Data Act.

> *Data saves lives*: This is a policy initiative to ensure better use of health data, including making health data available for research through the use of secure processing environments. It has some similarities to the EU's proposed European Health Data Spaces Regulation.

(cont. overleaf)



The UK approach to digital reform

(cont. from previous)

> *Product Security and Telecommunications Infrastructure Act 2022*: This Act, amongst other things, imposes a limited set of security obligations on internet connected products. It therefore has some similarities to the EU Cyber Resilience Act but is much weaker.

> *Telecoms (Security) Act 2021*: This contains broad and strong obligations on providers of a public electronic communications network or a public electronic communications service to secure their network. It also limits or prohibits the use of networking technology from certain designated vendors. While the EU is proposing a range of cyber instruments there is no direct EU equivalent to this Act.

> *Financial Services and Markets Act 2023*: The Act will, amongst other things, allow HM Treasury to designate certain suppliers as "critical". Designation means they will be subject to minimum resilience standards and testing, and the Financial Conduct Authority/Prudential Regulatory Authority will be able to obtain information as well as appoint skilled persons and investigators to review any resilience measures. This aspect of the Act is similar to the provisions in EU DORA to regulate critical third-party suppliers.

> *Online Safety Act 2023*: The Act will impose obligations on social media providers and search engines to protect users against illegal content. There are also some more limited provisions in relation to content that is lawful but harmful to children. This is similar to parts of the EU's Digital Services Act. The UK Information Commissioner has also issued an Age Appropriate Design Code (referred to as the Children's Code) which imposes online safety obligations to protect children.

> *Digital Markets, Competition and Consumers Act 2024*: This implements wide-ranging reforms to competition and consumer protection laws. The legislation will put the Digital Markets Unit on statutory footing and introduce a new regulatory regime for digital markets. Those additional powers to regulate digital markets have some similarity to the powers in the EU Digital Markets Act.

> *Cyber Security and Resilience Bill*: The Bill will strengthen the UK's cyber defences, ensure that critical infrastructure and the digital services that companies rely on are secure. There are likely to be parallels between this and NIS 2.0.

The overall UK approach is more limited and less interventionist, with greater reliance on policy initiatives and more targeted legislative initiatives. While the UK and EU regimes are currently aligned in many areas the UK is, over time, drifting apart.

Key contacts

Guillaume Couneson
Partner, Technology, Brussels
guillaume.couneson@linklaters.com
+32 2501 9305

Georgina Kon
Partner, Technology, London
georgina.kon@linklaters.com
+44 20 7456 5532

Ben Packer
Partner, Dispute Resolution, London
ben.packer@linklaters.com
+44 20 7456 2774

Daniel Pauly
Partner, Technology, Frankfurt
daniel.pauly@linklaters.com
+49 6971003 570

Edited by Peter Church and Federico Dante De Falco.

LLE!3001862232