TRAVERS SMITH

EU Digital Legislation:
What do you need to know?

Introduction

Since the publication of its report in early 2020 on the Shaping of Europe's Digital Future, the EU has proposed, and in some cases passed as law, a raft of EU legislation which deals with digital aspects of the economy – in effect, the EU's tech rulebook.

We set out here an overview of the key legislation and what you need to know about it. This will be particularly relevant if you are a digital business operating in the EU or supplying into the EU.

Data

- Data Governance Act
- European Data Act
- ePrivacy Regulation (draft)

Digital Services

- Digital Services Act
- Digital Markets Act

Cyber

- NIS II Directive
- Digital Operational Resilience Act
- EU Cyber Resilience Act (draft)

AI

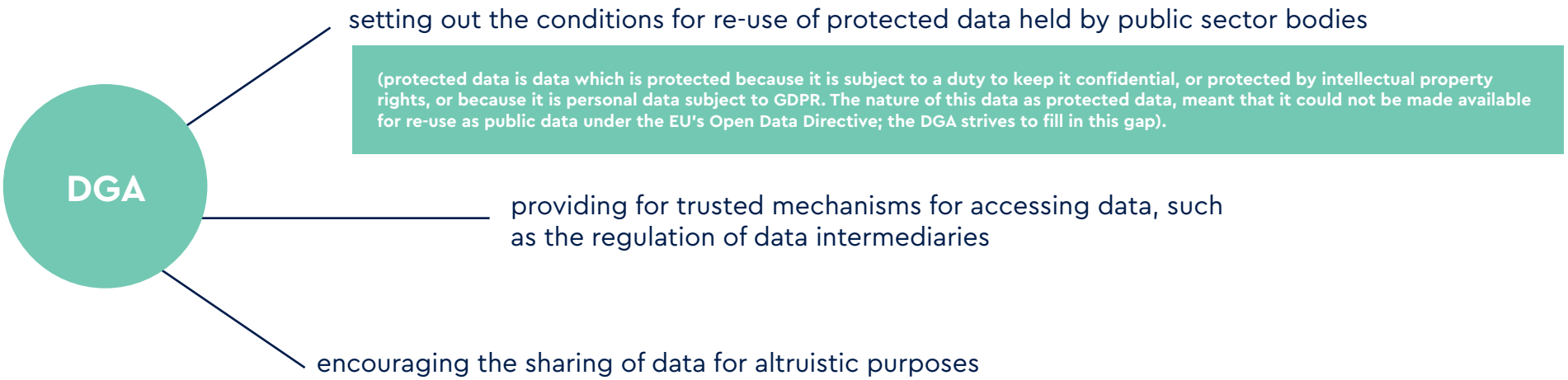
- AI Act (draft)
- AI Liability Directive (draft)

Data

Data Governance Act

What is it about?

The Data Governance Act (Regulation (EU) 2022/868) (the DGA), together with the European Data Act (see below), form part of the EU's strategy to encourage the sharing and re-use of digital data by allowing it to move freely within the EU and across sectors. The DGA contributes to this by:



The DGA applies to both personal and non-personal data, although the processing of personal data will still be subject to the General Data Protection Act (GDPR), where that applies.

Who (and what) does it apply to?

- Public sector bodies
- Anyone wishing to set up as a data intermediary
- Anyone wishing to set up as a data altruism organisation

a 'data altruism organisation', is a not for profit organisation which facilitates the voluntary sharing of data by individuals and companies for the benefit of society.

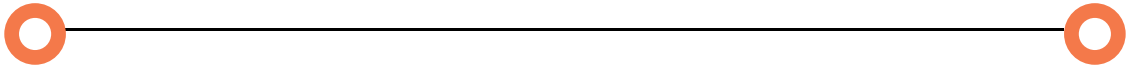
What does it do?

The DGA:

- **provides rules and safeguards to facilitate the re-use of protected data** held by public sector bodies (provided other legislation does not prohibit re-use of that data). The DGA does not positively require public sector bodies to share such data but rather sets out the safeguards which these bodies must employ if they do decide to share the data for re-use. Examples of these rules include that:
    - public sector bodies must have technical measures such as anonymisation and secure data access rooms in place to ensure that privacy and confidentiality of data is fully respected when it is re-used;
    - public sector bodies must assist potential re-users by trying to seek consent of individuals/dataholders to the sharing of their data, where consent for access is so required.
    - public sector bodies may only transfer confidential data, protected non personal data or data protected by intellectual property rights to a re-user intending to transfer that data to a third country outside the EU, if certain conditions are first put in place, such as contractual commitments from the re-user, and a declaration by the EC that the third country essentially provides protection to protected data, to an equivalent standard to that provided in the EU. (To the extent that protected data consists of personal data, than the GDPR rules on data transfers to third countries prevail).
- **sets out rules for those organisations wishing to provide data intermediation services** such as data market places, to ensure that they can function as trustworthy organisers of data sharing and as neutral third parties to connect individuals and companies with data users. Examples of these rules include a prohibition on data intermediaries monetising the data (thought they may charge for their data sharing services), and requirements on data intermediaries to avoid conflicts of interest.
- **encourages the voluntary sharing by individuals and companies** of the data they generate for general public interest use – 'data altruism', by setting up a common consent form to aid the collection of such data in a uniform format. Data altruism organisations wishing to act as brokers must be not-for-profit, operate transparently, and comply with a rule book which will set out technical and organisational measures that they will have to follow in relation to the data they collect and share.

A European Data Innovation Board will be set up to oversee all of this.

What is its current status?



23 June 2022
DGA came into force

24 September 2023
DGA applicable

As a regulation it has direct effect in the EU, though many provisions such as penalties for infringement are left for member states to determine.

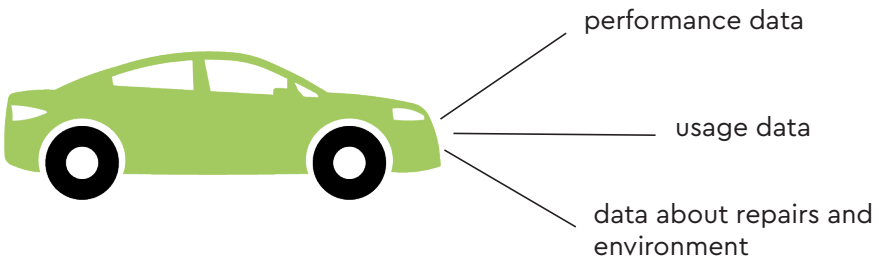
How you can prepare

The DGA creates a framework for facilitating greater data sharing and re-use, through laying the ground rules for public sector bodies to permit the re-use of the protected data that they hold. It also regulates those businesses and entities which wish to set up as data intermediaries or as recognised data altruism organisations. It will therefore be of limited direct application to the majority of businesses, unless they fall within this particular scope. However its objective to facilitate the sharing and availability of data means that it could prove useful for anyone who wishes to access and re-use data sets held by public sector bodies, companies with large data sets which want to share their data through a trusted data intermediary, and those sectors which might benefit from data altruism, such as scientific research projects.

European Data Act

What is it about?

Connected devices and the Internet of Things generate huge amounts of data (such as the examples in the diagram) which, as yet, are largely untapped. Whilst the Data Governance Act is intended to facilitate data sharing across sectors and member states, it does not create positive obligations on public sector bodies or other entities, to share data. This is left, to a certain extent, to the European Data Act (EDA), which is intended to unlock and maximise the commercial value of data, by specifying how it should be made available and to whom. It does this by introducing rights for companies and individuals to require that data holders make certain data available to them or to third parties in certain circumstances.



The EDA will also address a number of other issues related to digital data.

Who does it apply to?

The EDA will apply to manufacturers of connected devices that are placed on the EU market, suppliers of related services, data holders that make data available to data recipients in the EU, and providers of cloud services to customers in the EU.

What does it do?

The EDA:

- **gives users of connected devices access to the data which their use of the device generates**, whether for their own use or to share with third parties (e.g. for the purpose of carrying out repairs to a product) (please see bullet below for further details about the terms of such data sharing with third parties). Data holders such as manufacturers will have to make the data easily accessible, free of charge, without undue delay, and, where relevant, continuously and in real time. To complement this, there are transparency obligations on data holders, who must provide clear and concise information about the data they generate, what they do with it, and who they share it with.

- **regulates terms in data sharing contracts with third parties** to ensure that they are fair, reasonable and non-discriminatory. In particular, it sets out those terms in contracts between data holders and SMEs which will be regarded as unfair (intended to rectify the power imbalance between the two sides). The Act also mandates the European Commission to produce non binding model contractual terms and conditions for data use, and includes provisions on the amount of compensation which data holders can charge for sharing data with a third party: if the recipient is a company, then appropriate compensation can be demanded though it must be non discriminatory and reasonable; for sharing with SMEs or non profit organisations, the data holder may only re-charge its costs of sharing the data.

- **obliges data holders to provide public bodies with access to data** where this is needed on an exceptional basis, such as in relation to a terrorist attack or public health emergency.

- **sets out provisions to make it easier for customers to switch between providers of cloud data processing services**, and provides for the development of interoperability standards for data to be reused between sectors.

There are also provisions regulating the transfer of (non-personal) data outside the EU: data processing services providers (eg cloud service providers) will have to take all reasonable technical, legal and organisational steps, and put safeguards in place, to prevent the transfer of non personal data outside the EU where that could create a conflict with EU or national law (so for example, data in relation to national security or defence, or commercially sensitive information). In addition, there are restrictions on transferring data in response to third country access requests, and in some instances, a GDPR/Schrems II style transfer impact assessment of the third country's legal system would be required.

What is its current status?

11 January 2024
EDA comes into force

12 September 2025
Most obligations are applicable from this point

12 September 2026
Design obligations apply from this point

12 September 2027
EDA applies to certain contracts concluded on or before 12 September 2025

The EDA is a regulation and therefore is directly applicable in member states without the need for further enactment legislation.

How you can prepare

The EDA will directly impact manufacturers of connected products and cloud service providers in the EU.

Manufacturers will need to:

- ensure that products are designed with the EDA requirements in mind – e.g. to ensure that data can be securely accessed by, or made available on request to users, and can be shared easily and securely by users with third parties;
- revise product information to comply with the information and transparency requirements of the EDA;
- draft terms and conditions for their agreements with both data users and third parties with whom they share data, again ensuring that they comply with the requirements of the EDA.

Cloud service providers and other data processing service providers will need to make sure that they can comply with the contractual, commercial and technical requirements of the EDA to enable customers to switch more smoothly between providers. They will also need to identify their data transfers outside the EU and conduct due diligence to make sure that these do not conflict with EU or member state law. Conversely, customers should familiarise themselves with the termination and switching framework that the Data Act imposes on data processing service providers, so that they are well placed to benefit from the changes introduced by the Act.

For more detail, scan the QR code to read our briefing, '**EU Data Act – proposed rules for accessing and sharing data**'

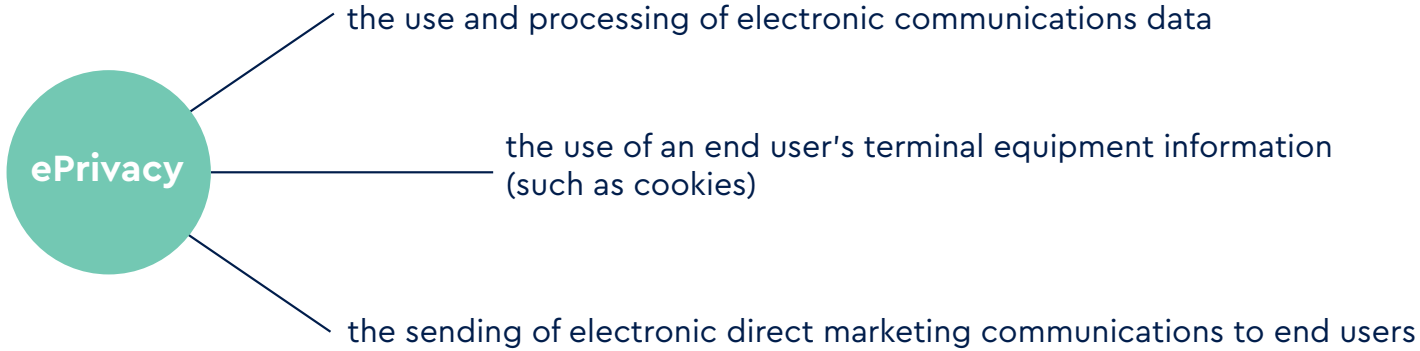
For more detail, scan the QR code to read our briefing, '**The EU Data Act: Scoping the impact for data holders**'

ePrivacy Regulation (draft)

What is it about?

The draft ePrivacy Regulation (the Regulation) is intended to replace the current Directive on Privacy and Electronic Communications. It sets out and updates the rules on protecting privacy and confidentiality when providing electronic communications services within the EU, in part to reflect the many changes in such services and the developments in new tracking and comms technology that have occurred since the Directive was first adopted. The new Regulation was intended to sit alongside the GDPR, however, its journey through the EU legislative process has not been straightforward.

Who/what does it apply to?



The Regulation applies to the provision of these services/the carrying out of these activities in the EU, and will therefore have extra-territorial effect.

What does it do?

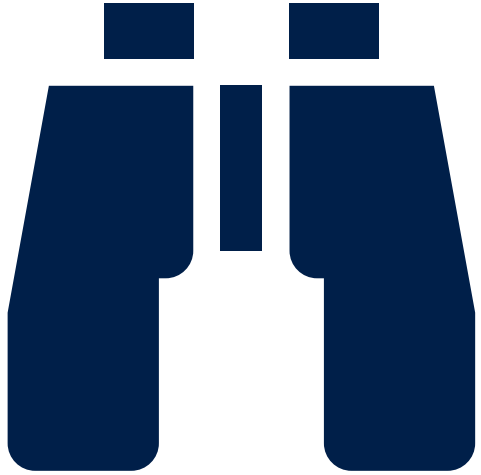
The Regulation:

- **provides a framework for protecting the privacy and confidentiality of electronic communications data (for example, text, photos, documents, text messages, Whatsapp messages) together with any associated transmission meta data.** It sets out the limited circumstances in which service providers may process or intercept such data (eg only if necessary to provide their services, or where processing is necessary for the security of the services, or compliance with the service provider's legal obligations under EU law).

- **sets out rules on the setting of cookies and similar technologies on end user devices**, when and how consent must be obtained (with the intention to simplify the current rules and provide a workaround for the perceived consent overload which has resulted from the current Directive).

- **reiterates the rules in the current Directive on the circumstances in which electronic direct marketing** can be carried out.

- **provides for GDPR-style sanctions** for breach, with fines up to the greater of a maximum of €20 million or 4% of annual worldwide turnover.



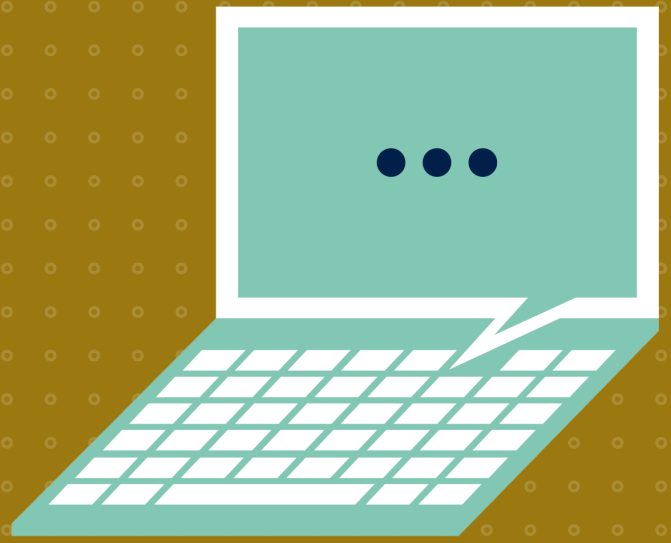
What is its current status?

The Regulation was intended to work alongside the GDPR, however, since its initial proposal in 2017, progress towards reaching agreement on a draft that keeps up with the rapid pace of technological developments in electronic communications has been slow. However, there will be a transition period of 24 months, as and when it is finally adopted.

How you can prepare

Electronic communications service providers will have to review their governance procedures to ensure that that they can comply with the rules on access to and use of content and metadata. Businesses may well also have to revise their practices regarding cookies and similar technologies, together with the circumstances in which they carry out electronic direct marketing so as to ensure compliance. However, the 24 month transition period should leave ample time for this.

Digital Services



Digital Services Act

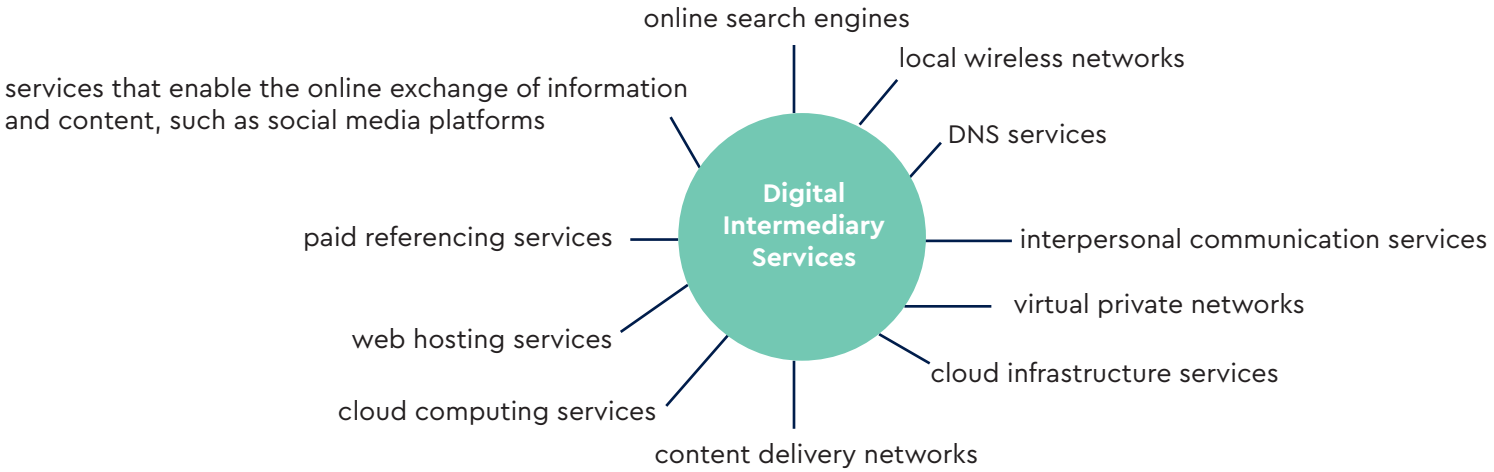
What is it about?

The Digital Services Act (Regulation (EU) 2022/2065) (the DSA), together with the Digital Markets Act, form part of the EU Digital Services Act package which is aimed at regulating the behaviour of online platforms and intermediaries, to make them more accountable for the way they operate in the market, and for the content on their platforms and the way that is curated.

The DSA regulates the way in which online/digital intermediaries provide their services, and is intended to harmonise the rules within the EU on the safety of online services and the dissemination by intermediaries of illegal content online.

Who does it apply to?

- The DSA applies to digital intermediary services (ISPs), which are defined as conduit, caching and hosting (including online platform) services. These include:



- The DSA will have extra-territorial effect as it applies to intermediary services offered to recipients in the EU regardless of where the ISP is based.

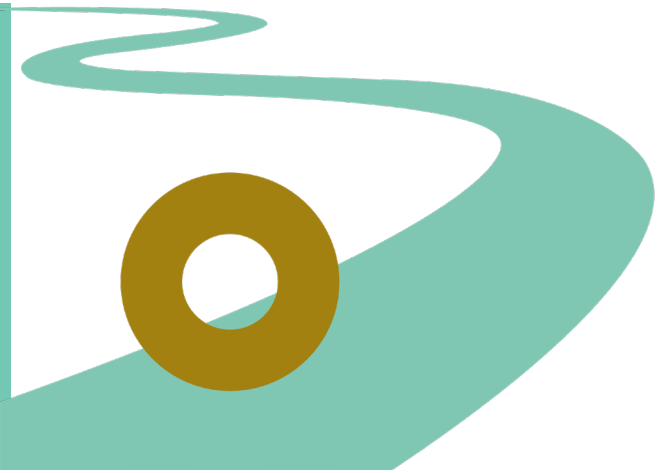
What does it do?

The DSA:

- **establishes a framework for the conditional exemption from liability of providers of intermediary services.** It echoes the intermediary defences set out in the eCommerce Directive (essentially, providing exemptions from liability for those ISPs which play a neutral role in carrying out their services).
- **prescribes specific due diligence, risk assessment, accountability and transparency obligations** aimed at improving the management of risks arising from illegal online content and other online 'harms' such as recommender systems and targeted advertising. These are tailored to specific categories of intermediary service providers.
- **applies specific rules to online consumer market places**, for example, the requirement for online market places to carry out greater checks on the traders which use their platform to ensure their traceability (Know Your Business Customer Due Diligence).
- **imposes fines** of up to 6% of annual worldwide turnover for breach.

The obligations work cumulatively depending on the type and size of service you are, with the most stringent rules reserved for 'very large online platforms' (VLOPs) and 'very large search engines', (VLOSEs) defined as online platforms and search engines which have at least 45 million active monthly service recipients in the EU, and designated as such by the European Commission. An initial list of VLOPs and VLOSEs was designated by the Commission in April 2023, and includes the "Big Tech" platforms such as Facebook, Amazon, Instagram, Twitter, YouTube, Bing, and Google Search.

There are baseline obligations that apply to all ISPs for example requirements to appoint a point of contact, and in the case of those providers established outside the EU, an EU member state-based legal representative, and to ensure that their terms and conditions include information about their content moderation processes. VLOPS and VLOSEs face many additional obligations for example, rules on transparency in relation to targeted advertising, requirements to set up an internal compliance function, and carry out risk assessments in respect of illegal content.



What is its current status?

November 2022
DSA entered into force entities

February 2023
Platforms and search engines published user numbers

April 2023
VLOPs and VLOSEs were designated with compliance required after 4 months

February 2024
DSA applies to all regulated entities

The DSA is a regulation and therefore is directly applicable in member states without the need for further enactment legislation.

How you can prepare

- If you are an online business, consider whether you are within scope – because of the type of digital services which you provide, and because those services are essentially aimed at EU based customers.
- If you are in scope, identify which category of ISP you fall within (and therefore the level and nature of compliance that you'll need to meet).
- If necessary, carry out an audit to establish what technical, organisational and legal changes need to be made internally and to your website/online platform.

For more information on the DSA, scan the QR code to see our briefing.

Digital Markets Act

What's it about?

The Digital Markets Act (Regulation (EU) 2022/1925) (the DMA) aims to regulate unfair and anti-competitive behaviour of large internet companies. Whilst EU competition law also continues to apply, the DMA provides an additional layer of regulation which takes into account the specific nature of the digital market.

Who does it apply to?

The DMA focusses on large online companies (essentially 'big tech' businesses) which provide 'core platform services', known as 'gatekeepers' within the DMA. There are detailed provisions which will help online companies to identify whether they provide a core platform service and are considered a 'gatekeeper' under the DMA.

What is a core platform?

Examples of core platform services include online search engines, online social networking services, video platform sharing services, and cloud computing services – in other words, businesses which essentially act as gateways between business users and consumers.

What is a gatekeeper?

To be considered a gatekeeper, these platforms have to be of a size which has the potential to have a significant impact in the EU internal market; a rebuttable presumption is created if the platform hits a certain size threshold – it must have a market capitalisation of at least €75 billion or an annual turnover of €7.5 billion, and have at least 45 million monthly end users in the EU and 10,000 annual business users.

What does it do?

Gatekeepers will have to comply with a series of do's and don'ts set out in the DMA which are aimed at ensuring that they do not abuse their position in the market and, keeping digital markets fair and 'open' for market participants. For example, there are requirements on gatekeepers to allow third parties to inter-operate with the gatekeeper's own services, and to allow businesses to access the data which they generate in their use of a gatekeeper's platform, and there are prohibitions on preventing customers from linking up to businesses outside a gatekeeper's platforms, and preventing users from uninstalling pre-installed software or an app if they wish to do so.

Breach of the DMA can result in fines of up to 10% of a company's worldwide annual turnover, or up to 20% for repeated infringements. By way of an 'incentive' to comply, there is also provision for periodic penalty payments of up to 5% of average daily turnover for failure to comply with measures specified by the Commission in a decision, or where a gatekeeper does not co-operate with the Commission's investigations.

What is its current status?

The DMA came into effect in November 2022; most provisions started to apply in May 2023, and the Commission designated six companies as 'gatekeepers' on 6 September 2023: Amazon, Apple, Meta, ByteDance, Microsoft and Alphabet. Subject to appeals and the outcome of two market investigations that the Commission has agreed to carry out, these companies now have six months to submit detailed compliance reports.

How you can prepare

The Commission will be able to designate more gatekeepers as market conditions evolve, which means that those core platform services which are heading towards meeting the size thresholds should keep a close eye on developments. For other players in the market, it's useful to know that this legislation does now exist for keeping big tech companies in check in the EU.

Cyber

NIS 2 Directive

What is it about?

The NIS 2 Directive (Regulation (EU) 2022/2555) (NIS 2) is the EU's next generation version of the Network and Information Systems Directive, updated to respond to the growing threats posed by digitalisation and the surge in cyber attacks, as well as addressing some of the perceived shortcomings of the first directive. Like its predecessor, NIS 2 aims to establish a higher level of cybersecurity and resilience within EU-based organisations of a certain size, and which operate in named sectors which are regarded as critical or very critical, by strengthening minimum security requirements, addressing security of supply chains, streamlining reporting obligations and introducing more stringent supervisory measures. A greater breadth of sectors are caught by NIS 2 than its predecessor and there's a greater emphasis on uniform transposition into local laws across EU member states to correct some of the inconsistencies created by the first directive.

Who does it apply to?

NIS 2 applies to "large" and "medium" sized entities which offer services in the EU and operate in "very critical" and "critical" sectors.

Very Critical

- Energy
- Transport
- Banking
- Infrastructure for the financial market
- Health care
- Drinking water
- Wastewater
- Digital infrastructure
- Management of ICT services
- Government
- Space travel

"Large" sized entity	=	>250 employees + earns at least €50 million
"Medium" sized entity	=	>50 employees + earms at least €10 million

Critical

- Postal and courier services
- Waste management
- Manufacture, production and distribution of chemicals
- Production, processing and distribution of food
- Manufacture
- Digital products
- Research

A further categorisation is between "essential" and "important" entities, and this affects the way in which an entity is supervised and regulated under NIS 2. An entity will only be treated as "essential" if it is "large" and operates in a "very critical" sector. Other "large" entities in "critical" sectors will just be treated as "important", as will "medium" sized entities operating in "very critical" or "critical" sectors. There are exceptions: – some entities will be considered "essential" regardless of size, if a service outage would have serious consequences to society or they are the exclusive national provider, including entities which provide public communications network services.

What does it do?

NIS 2:

- **strengthens cybersecurity requirements for organisations by:**
    - providing a minimum list of basic technical and organisational measures which should be instigated, such as implementing policies for IS security and incident response and making use of cryptography and encryption;
    - requiring organisations to review cybersecurity risks in their supply chains (including those located outside the EEA);
    - introducing governance and accountability obligations on management boards (with failure to comply resulting in potential liability for senior management).
- **expands incident reporting obligations**, which will be tiered depending on the severity of the incident.
- **requires member states to identify essential and important entities** within scope by 7 April 2025 (which effectively means that entities will have to register in each member state in which they provide in-scope services).
- **provides for more stringent supervisory measures for authorities together with enhanced co-operation mechanisms for member states.**
- **'subjects' 'essential' entities to a maximum fine of €10 million or 2% of annual global turnover, and 'important' entities to a maximum fine of €7 million or 1.4% of annual global turnover, in each case, whichever is the greater.**

What is its current status?

16 January 2023
NIS 2 entered into force

17 October 2024
Member states must have transposed NIS 2 into their national legislation

18 October 2024
Member states must start applying the law

How you can prepare

- Identify if your organisation is likely to be in scope, based on the type of services which it provides, whether it provides them in the EEA, and whether it meets the size thresholds.
- Audit your systems and processes to assess whether they comply with NIS 2 requirements, identify any issues that need addressing, and ensure that you have appropriate processes, policies and procedures in place.
- Identify your key business critical IT suppliers and audit them to identify and address cybersecurity risks. Whilst not directly impacted, suppliers should be prepared for increased due diligence from in-scope NIS 2 organisations, in respect of their cybersecurity and information security policies and procedures.

Scan the QR code to read our briefing,
'**Strengthening cybersecurity laws: changes to the EU's and the UK's NIS regimes**'

The Digital Operational Resilience Act

What is it about?

Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) prescribes requirements for digital operational resilience and information and communication technology (ICT) risk management in the financial services sector. It also consolidates and upgrades the ICT risk requirements in other separate pieces of EU legislation.

Who does it apply to?

DORA applies to EU financial services institutions. Such as...

central securities depositories, central counterparties, trading venues, MiFID investment firms, payment institutions and e-money institutions

DORA also regulates their critical third party ICT service providers.

What does it do?

Requirements include:

- **ICT risk management** such as identifying all sources of ICT risk and setting up a framework for risk management, together with systems and tools to minimise the impact of ICT risk; protection and prevention measures to prevent loss of data and information leakage; measures to detect anomalous activities; a comprehensive business continuity policy and disaster recovery plan.
- **digital operational resilience testing** with regular independent testing of critical ICT applications and systems.
- **implementation of a management process to detect and manage ICT related incidents** and report them to relevant authorities where necessary.
- **good governance:** an institution's management will be directly responsible for managing ICT risk.
- **pro-active management of ICT suppliers** including carrying out due diligence and risk assessments, managing those risks, and putting in place appropriate contract documentation (the terms of which are heavily prescribed by DORA). Designated critical ICT third party providers will be subject to direct oversight by applicable EU supervisory authorities.

What is its current status?

16 January 2023
DORA entered into force

17 January 2025
DORA will apply

How you can prepare

Financial institutions which are within scope of DORA should use the implementation period to embed digital resilience at all levels of their operations. They should audit their systems, processes, policies and procedures to identify shortfalls against the requirements of DORA and put together a plan for compliance. ICT suppliers to EU financial institutions will need to be prepared to be subject to greater due diligence in this regard, and to amend the terms of their supply contracts so that they comply with DORA.

EU Cyber Resilience Act (draft)

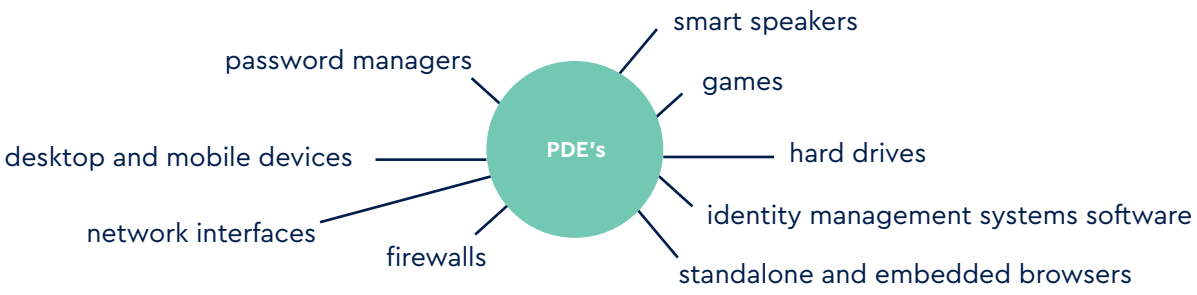
What is it about?

The EU Cyber Resilience Act (the CRA) sets out the EU's framework for tackling cybersecurity risks in connected products (i.e., hardware, software and their remote data processing solutions as well). Broadly, the framework addresses cybersecurity in three ways:

- Imposes obligations on manufacturers to design, develop and produce connected products that have fewer vulnerabilities;
- Ensures that manufacturers remain responsible for cybersecurity throughout a connected product's life cycle by imposing requirements for vulnerability handling processes;
- Sets out the rules for market surveillance and enforcement.

Who (and what) does it apply to?

The CRA applies to "products with digital elements" that connect to another device or network ("PDE") placed on the market in the EU, and will be of relevance, primarily to the manufacturers of such products, but also to those importing or distributing products on the EU market. The CRA applies to all hardware and software connected to the internet, together with their remote data processing solutions; any related software which is needed in order for such products to operate, and any components which will be integrated into such products. Examples of PDE's include:



(There are exceptions – medical and in-vitro medical-diagnostic devices are excluded from scope as well as motor vehicles, because sector specific legislation already regulates the management of cybersecurity risks for these products. Connected products developed exclusively for military or national security purposes, or specifically to process classified information, are also excluded.)

What does it do?

Under the CRA **manufacturers** must:

- **carry out cybersecurity risk assessments and address these** during the planning, design, development, production, delivery and maintenance phases of the PDE's life cycle, with a view to minimising cybersecurity risks, preventing security incidents and minimising the impact of such incidents.
- **carry out due diligence when sourcing third party components** to ensure that these do not compromise the cybersecurity of the product.
- **ensure that products are designed, developed and produced to meet the 'essential' cybersecurity requirements set out in the CRA**, including protecting against unauthorised data access; designing, developing and producing products to limit denial of service attacks; including a secure by default configuration, and ensuring that vulnerabilities can be addressed through security updates. Manufacturers will have to carry out conformity assessments to test whether their products meet these essential requirements and produce technical documentation to show how they conform.
- **ensure that product vulnerabilities are handled effectively during the expected lifetime of the product**, or if shorter, a period of 5 years from placing the product on the market, including by identifying vulnerabilities, applying regular testing, providing security updates, and providing a mechanism for vulnerabilities to be reported.
- **report security incidents** (and comply with related requirements) to the EU Agency for Cybersecurity and to users.

Importers and **distributors** will have to carry out due diligence before importing or placing PDE's on the EU market to ensure that a conformity assessment has been carried out, amongst other things. There are also reporting obligations in relation to identified cybersecurity risks, to the manufacturer, and in some cases, relevant authorities.

Each member state will have to appoint a market surveillance authority to supervise and enforce the CRA at national level. There will also be a pan-European dedicated co-operation group to ensure the consistent application of the CRA in member states. Fines for breach range from the greater of €5–15 million, or 1 to 2 % of worldwide turnover in the preceding year.

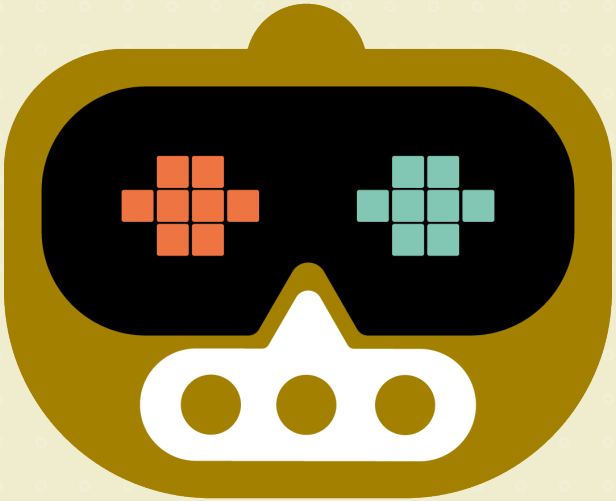
What is its current status?

The European Parliament and the Council reached political agreement on the draft CRA in December 2023. The agreement is now subject to formal approval by both the European Parliament and the Council, likely to be in April 2024. There will be a 36-month transition period for products to be adapted to the new requirements with the exception of a more limited 21-month grace period in relation to the reporting obligation of manufacturers for incidents and vulnerabilities.

How you can prepare

For many tech manufacturers, many of the essential requirements of the CRA for dealing with cybersecurity risks may well already be baked into their products, with only some fine-tuning required for new products to conform. Manufacturers should start familiarising themselves with the broad baseline requirements and consider how these can be incorporated into their design and development processes and, where necessary, up their supply chains (for third party components).

AI



AI Act (draft)

What is it about?

The AI Act will regulate the development, deployment and use of AI in the EU, and the way in which associated risks are managed. The rules in the Act are intended to ensure that AI developed and used in the EU is in line with EU rights and values such as human oversight, safety, privacy, transparency, non-discrimination and social and environmental wellbeing.

Who does it apply to?

The Act applies to manufacturers, suppliers, importers and deployers of AI in the EU. It also applies to anyone whose AI systems produce output used in the EU. Note that some 'high risk AI systems' (see below) which are already subject to existing EU product safety regulation (eg in sectors such as civil aviation, motor vehicles, agriculture and forestry vehicles, rail systems and marine equipment, machinery, medical devices, toys, lifts, radio equipment) will be treated differently and will continue to fall under existing conformity frameworks rather than the AI Act.

What does it do?

The Act creates a tiered approach to risk:

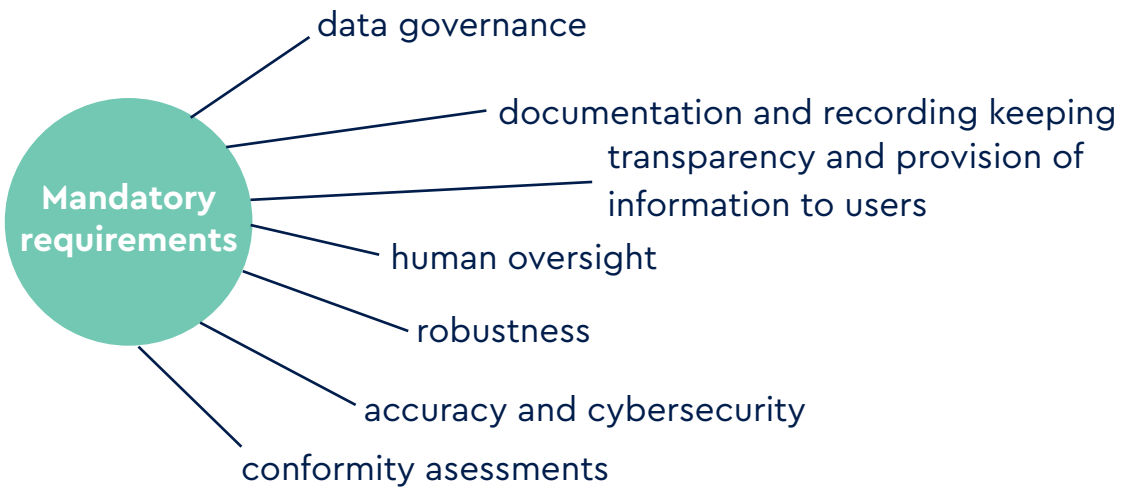
- there is an outright ban on those systems which are classified as 'unacceptable use' systems – or in other words, those systems which are considered to violate fundamental rights.

e.g. systems for social scoring, harmful behavioural manipulation, real-time biometric identification (RBI) systems for law enforcement purposes (subject to narrow exemptions), predictive policing, emotion recognition systems in law enforcement, border management, workplace and educational institutions, scraping of biometric data from social media or CCTV footage to create facial recognition databases

- 'high risk' systems – or in other words, those systems which can potentially have a negative impact on people's safety or their fundamental rights (eg systems used as safety components for certain products; RBI in public spaces (outside of banned contexts); the use of AI for employment assessment, education, management of critical infrastructure and certain public functions) will have to comply with mandatory requirements (see diagram).

- 'limited risk' systems (eg systems which are used in human interactions such as chatboxes, emotion recognition (outside of banned contexts) or 'deep fake' creation) will only be subject to specific transparency obligations, such as making people aware of when they are being used and to the 'core' AI principles described below.

- 'minimal risk' systems won't be subject to any obligations.



There will also be a 2-tier risk system for general purpose AI models:

1. Providers of all general purpose AI models (other than those which are open source) are expected to comply with certain transparency obligations, measures to ensure copyright law has been adhered to and requirements to publish a sufficiently detailed summary of data used to develop the model;

2. Rules that apply to particularly powerful, "systemic" models. Their providers will have to conduct model evaluations, assess and mitigate systemic risk, conduct adversarial testing, report to the Commission on serious incidents, ensure cybersecurity and report on their energy efficiency.

Six high level core principles will apply to all AI systems regulated by the AI Act. These are:

- Human agency and oversight
- Technical robustness and safety
- Privacy and data governance
- Transparency
- Diversity, non-discrimination and fairness
- Social and environmental well being

Proposed sanctions for non compliance include penalties of up to the greater of 7% of annual global turnover or €35 million for the most serious breaches. National regulators will oversee compliance, but a European Artificial Intelligence Board comprising representatives of member states from these regulators will be set up to oversee the implementation of the Act and to ensure consistency.

What is its current status?

The draft Act received its final assent from the EU Parliament on 13 March 2024. Minor linguistic changes are still to be approved by the EU Parliament and, thereafter, the final approved version will be published in the Official Journal of the EU. It will enter into force 20 days after publication (likely to be May 2024). It will apply two years after its entry into force, except for some specific provisions which will come into effect earlier: bans will apply after 6 months and the rules for general purpose AI will apply after 12 months.

How you can prepare

Although the AI Act has not been finalised, there are measures which an organisation in scope can take in order to gain a head start when it comes to compliance:

- Identify the AI systems which your organisation uses and how they are used, to establish which risk approach would apply to them. Create a register to map this out.
- Carry out an AI risk assessment (like a Data Protection Impact Assessment) to help identify potential risks associated with the AI, such as bias and discrimination, and how those risks can be mitigated.
- Maintain an effective audit trail of the data inputted into AI tools, the purpose for which it is being used, and any decisions taken on the basis of the output.
- Ensure there is appropriate human oversight when using AI tools.
- Think about transparency – what you need to tell people about when AI is being used, and the purposes for which it is being used.
- Address acceptable use in employee and supply chain policies.
- Bear in mind that other legislation such as the GDPR (e.g. where processing personal data) may already apply to how you use and develop AI, so an holistic approach to compliance will need to be adopted.

For further information scan the QR codes to read our briefings below:

'**The Shifting Sands of AI Regulation**'

'**AI tests intellectual property boundaries**'

'**Artificial intelligence: what role for data protection?**

'The UK's approach to AI regulation – an update

AI Liability Directive (draft)

What is it about?

The proposed AI Liability Directive (the Directive) aims to make it easier for claims to be brought for harm caused by AI systems and the use of AI, and is intended to complement the AI Act.

Who does it apply to?

The Directive will apply to providers, users and operators of AI systems which are available or operate within the EU.

What does it do?

The Directive:

- **lowers the evidential hurdles** for victims injured by AI related products or services.
- **introduces measures to empower EU member state courts** to compel disclosure of evidence about AI systems in certain situations (eg where those AI systems are classed as 'high risk' systems under the AI Act).
- **allows claims to be brought** by a subrogated party or representative of a claimant, including class actions.
- **introduces a presumption of causation** between the defendant's fault and the damage caused to the claimant by the AI system, which would apply if:
    - the claimant shows that the defendant failed to comply with a duty of care intended to protect against the damage, including (in the case of 'high risk' systems under the AI Act) a failure to comply with relevant obligations under the AI Act;
    - it can be considered reasonably likely that the fault influenced the output of the AI system/the AI system's failure to produce an output;
    - the claimant has shown that the output of the AI system or the system's failure to produce an output gave rise to the damage.

What is its current status?

The Directive was proposed in 2022 and will be considered by the European Parliament and the European Council. As a directive, it will not have direct effect in the EU once it is agreed and adopted, but will then need to be transposed into law by EU member states.

How you can prepare

The Directive underlines the importance of taking the steps outlined above to ensure compliance with the AI Act, once that comes into effect.

Get in touch

The Technology & Commercial Transactions team at Travers Smith has considerable expertise and experience in advising on issues relating to the application of technology and data law and regulation.

Please feel free to get in touch.

Dan Reavill
Head of Technology & Commercial Transactions
dan.reavill
@traverssmith.com
+44 (0) 20 7295 3260

Louisa Chambers
Partner, Technology & Commercial Transactions
louisa.chambers
@traverssmith.com
+44 (0) 20 7295 3344

James Longster
Partner, Technology & Commercial Transactions
james.longster
@traverssmith.com
+44 (0) 20 7295 3496

Clients include:

Matterport™ monzo access SAMSUNG ZPG TOYOTA connected

TRAVERS SMITH

*This publication is intended merely to highlight issues and not to be comprehensive, nor to provide legal advice. Should you have any questions or comments on issues reported here, please contact one of your regular contacts.

+44 (0) 20 7295 3000

10 Snow Hill, London EC1A 2AL
traverssmith.com