NORTON ROSE FULBRIGHT

European digital and cyber regulation

Contents

Introduction

In 2020, the European Commission (the Commission) published its central digital policy document "Shaping Europe's Digital Future" which outlined its digital strategy for the next five years. The Commission outlined concerns raised by the fact that people are increasingly living their lives online and the potential for certain online platforms to compromise the fairness and openness of EU markets.

The Commission's approach to shaping Europe's digital future is based on the following three main pillars, which are designed to enable control over the digital transformation:

1. Technology that works for people, which includes aims to protect people from cyber threats and ensure Artificial Intelligence (AI) is developed in ways that respect people's rights;
2. A fair and competitive digital economy, namely to facilitate fair competition for all companies in Europe and increase access to high-quality data; and
3. An open, democratic and sustainable society in which citizens are given more control over their data, "data spaces" for research, diagnosis and treatment purposes are created, disinformation online is addressed and diverse and reliable media content is fostered.

Reflecting its overarching strategy, the Commission also published a package of proposals entitled "Europe fit for the Digital Age" which provide more detail on how these objectives will be achieved.

This document examines some of the key EU legislation in that package, focusing primarily on legislation concerning data, cyber-security and AI. It also discusses and compares similar proposals/initiatives in the UK.

Please note that a number of the laws discussed in this document are still moving through the legislative process and therefore our summaries and conclusions are subject to change.

For further information on any aspects of this document please contact Marcus Evans and Lara White.

Marcus Evans
EMEA Head of Information governance, privacy and cybersecurity
Tel +44 20 7444 3959
marcus.evans@nortonrosefulbright.com

Lara White
Partner
Tel +44 20 7444 5158
lara.white@nortonrosefulbright.com

AI Act

The AI Act (AIA) is the EU's first comprehensive legislation setting harmonised rules regulating Artificial Intelligence and will impose new and significant obligations on those developing and using AI inside and outside the EU. The UK is also exploring the future regulation of AI.

Name of law

Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828.

What is the general purpose of the law?

The purpose of the AIA is to promote uptake of human-centric and trustworthy AI, and to ensure protection of health, safety, fundamental rights, democracy and the rule of law and the environment from the harmful effects of AI.

Is the text finalised yet? If not, when do we expect it to be finalised and apply from?

Yes, the full text is now available.

Prohibitions (outlined below) are likely to apply before the end of 2024. Provisions on general purpose AI are likely to apply by mid-2025. Most other provisions will likely apply from mid-2026 (though some provisions are likely to apply from mid-2027).

We will know the exact dates when the final procedural steps are completed and the AIA is entered into the EU's Official Journal, which is likely to take place around May 2024. 20 days from that date, the AI Act will 'enter into force', marking the beginning of a transitional period.
The provisions on prohibitions as well as provisions requiring organisations to promote AI literacy will apply (i.e. become enforceable) six months from this date.

The AIA has some retrospective effect:

- Operators of existing AI systems (that is, in place before the AIA) as components of large-scale IT systems related to border control and judicial cooperation must comply by December 31, 2030.
- Operators of existing high-risk AI systems (that is, in place before the relevant provisions of the AIA begin to apply) must comply where substantial modifications are made after AIA applies.

Who does the law apply to?

The AIA applies to all those who develop, distribute, and use AI systems that will affect people in the EU.

Most of the obligations under the AIA fall on providers, vendors who develop the AI systems. Deployers who use the AI systems must also comply with some obligations around their use, and some obligations also fall on importers and distributors who put AI systems on the market or into service in the EU.

Providers supplying the EU market must comply regardless of whether they are located in the EU.

Providers or deployers outside the EU must also comply where the output of the AI systems is to be used in the EU.

The Act regulates AI systems. An AI system is one which "for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions". An ability to infer is key; software will not necessarily be caught simply because it can apply logic or make predictions. 'General purpose AI models', which are trained on large amounts of data and capable of performing a wide range of distinct tasks, are also regulated.

What are the main provisions in the law?

The AIA adopts a "risk-based approach", setting out obligations in proportion to the perceived harms that can be caused by AI systems and models.

Prohibited AI practices

The AIA prohibits certain AI practices for which the EU institutions considered the level of risk to be unacceptable. Banned practices include:

- Subliminal/manipulative/deceptive techniques;
- Exploitation of the vulnerable;
- Biometric categorisation of sensitive/protected characteristics;
- Social scoring based on an unrelated social context or disproportionate to the social behaviour;
- Real-time remote biometric identification in publicly accessible spaces for law enforcement (outside of specific exemptions);
- Risk assessments to predict the likelihood of a person committing a criminal offence;
- Creation of facial recognition databases through untargeted image scraping; and
- Emotional recognition in the workplace or educational contexts.

High-risk AI systems

These are AI systems that create health and safety risks or risks to fundamental rights.

AI systems intended to be used as safety components of products like medical devices or protective equipment, that are already highly regulated under EU law, fall into this category. The obligations for these types of AI systems will apply from 36 months from 'entry into force', so are likely to apply from mid-2027.

Otherwise, AI systems can fall into the high-risk category where they meet certain criteria in the areas of biometrics, critical infrastructure, education, employment, essential private and public services and benefits, law enforcement, migration, asylum and border control management, and administration of justice and democratic processes.

These criteria are set out in Annex III to the AI Act. The obligations for AI systems caught by Annex III apply from 24 months from 'entry into force', i.e. most likely from mid-2026.

Examples of AI systems caught by Annex III include:

- Remote biometric identification
- Emotional recognition not falling under the prohibited practices;
- Recruitment, promotions, or termination of employees;
- Evaluating creditworthiness or establishing a credit score; and
- Risk assessment and pricing for life and health insurance.

Systems are exempted where there is no "significant risk" of harm to the health, safety or fundamental rights of natural persons. AI systems falling within the 'Annex III' list of high-risk practices cannot benefit from this exemption where they carry out profiling of natural persons. This proviso does not appear to have been intended to capture online advertising, as the Commission's Q&As confirmed that recommender systems of very large online platforms are not included, as they are already covered in the Digital Markets Act and Digital Services Act.

Provider requirements for high-risk AI systems
Providers of high-risk AI systems will be subject to numerous obligations. This is because the Commission and lawmakers consider them best placed to put safeguards in place during the technology's creation.

These include the following substantive requirements:

- Implementing a risk and quality management system covering all the typical areas over the AI development cycle: data appropriateness and quality, accuracy, explainability, oversight, robustness, fairness.
- Providing instructions for use to the deployer.
- Implementing a post market monitoring system, including capturing and retaining event logs.
- Eliminating or reducing risks to health, safety and fundamental rights such that the residual risk is judged acceptable.

- Keeping documentation, including detailed descriptions of the system itself, the development methodology, design choices, system architecture, datasheets, assessment of human oversight measures, validation and testing procedures and test logs to test for accuracy, robustness and discriminatory impacts (SMEs may provide this information in a simplified manner).
- Drawing up a declaration of conformity, which can be made by the provider or a conformity assessment body.
- Registering the AI system in an EU database.

Deployer requirements for high-risk AI systems
Deployer obligations include taking technical and organisational measures to ensure the provider's instructions are followed, ensuring appropriate and competent human oversight, and consulting with workers where they are affected.

In addition, deployers must undertake a fundamental rights impact assessment where they are that are bodies governed by public law or private operators providing public services, or where they are deploying an AI system to assess creditworthiness or carry out pricing or risk assessments for life and health insurance.

General purpose AI models (GPAIs)

As mentioned above, these are AI models trained on broad data at scale, which display significant generality of output, to and competency to perform a wide range of tasks. They are typically systems intended to perform functions like image and speech recognition, audio and video generation, pattern detection, question answering and translation which may be used in high-risk AI systems.

Providers of GPAIs must draw up and maintain technical documentation of the model, training and testing process and results of its evaluation and energy consumption. They must provide such technical documentation to providers of AI systems who intend to integrate a GPAI in their system.

Providers must also put in place a policy to respect EU copyright law and a summary of the content used to train the model.

GPAIs with systemic risk
A GPAI will be classified as having systemic risk if it (a) has "high-impact capabilities" or (b) the Commission makes a decision designating it as such. A GPAI will be presumed to have high impact capabilities if the cumulative amount of compute used for its training measured in floating point operations is greater than 10^25.

A provider must notify the Commission within two weeks of meeting the above criteria. It may accompany this notification with arguments that the GPAI does not present systemic risks because of its specific characteristics.

In addition to the obligations on GPAI providers, providers of GPAIs with systemic risk must provide evaluation strategies and results, undertake adversarial testing, mitigate systemic risks, document and disclose serious incidents and ensure adequate levels of cyber security.

Transparency obligations

Transparency obligations apply under the AI Act in some situations where lawmakers considered it important to flag that content was AI generated or a user was interacting with an AI system. These obligations are sometimes described as applying to AI systems that present 'limited risk,' though in practice they cut across other categories and can apply to high-risk AI systems, general purpose AI models, or AI systems that would otherwise be considered 'minimal risk.'

Providers must ensure that their systems inform individuals they are interacting with an AI system when it is intended to interact with individuals. They must also ensure AI generated content is watermarked where their systems can generate audio, images, video, or text. Deployers must inform individuals where they are using emotion recognition, and must disclose where they are using AI generated or manipulated content (to ensure "deep fakes" are flagged). They must also disclose where text has been artificially generated, unless reviewed by a human.

Minimal risk AI systems

This is a term used to describe AI systems include applicationsthat are not high-risk and do not use general purpose AI models, like AI-enabled video games or spam filters. The AIA encourages providers of these systems to apply voluntary codes. Providers and deployers must take measures to ensure a sufficient level of AI literacy "to their best extent".

The role of standards and specifications

Standards

Standards will be highly important
Adherence will be a major factor in demonstrating compliance with the AIA. Presumption of conformity

High-risk AI systems and general purpose AI models in conformity with harmonised standards ("harmonised standard" means a European standard published in the Official Journal) are presumed to be in conformity with various requirements.

Common specifications

Where harmonised standards are not available, the Commission can create a common specification for compliance with requirements and obligations for high-risk and general purpose AI. The following provisions apply:

Presumption of conformity
High-risk AI systems in conformity with common specifications are presumed to be in conformity with the relevant requirements of the AIA.

Justify non-compliance
Where providers of High-risk AI systems are not compliant with common specifications, they must justify that they have adopted technical solutions to an equivalent level.

Who will enforce the law?

The AIA introduces a dual governance system at Member State and EU level.

At the EU level:

- The Commission will have enforcement powers against general purpose AI models, acting through a new AI Office.
- The AIA creates an EU AI Board, responsible for providing guidance and promoting a harmonised approach to enforcement, much like the European Data Protection Board. Its membership will comprise one representative per of Member States, with the European Data Protection Supervisor participating as an observer.
- There will also be an EU Advisory Forum, which will provide the Commission and AI Board with technical expertise.

The European Commission will also have delegated legislative power under the AIA to update/make certain changes to it and to issue guidance.

Each Member State must also designate at least one:

Notifying Authority
A national authority responsible for appointing conformity assessment bodies and their supervision.

Market Surveillance Authority
Market surveillance authorities are responsible for enforcement (other than in relation to general purpose AI models). The market surveillance authority could be an existing sectoral or cross-sectoral regulator, or responsibility could be shared between more than one regulator. The AIA specifies a default position in some cases, for example, the financial services regulator will general be the market surveillance authority in relation AI systems used in financial services, but derogation from this default position is permissible where justified.

While no AIA market surveillance authorities have been formally appointed in writing, it is likely that the data protection authorities will take on the role in both France and the Netherlands.

What are the consequences of non-compliance with the law?

Member States will be required to lay down rules on penalties, with a hierarchy of fines applying depending on the severity of the infringement. The AIA prescribes the following maximum requirements:

Non-compliance with prohibited AI practices
Up to €35m or seven per cent of the total worldwide annual turnover of the preceding financial year (whichever is higher) for infringements on prohibited practices or non-compliance related to requirements on data.

Non-compliance with other requirements
Most provisions carry a penalty of up to €15m or three per cent of the total worldwide annual turnover of the preceding financial year for non-compliance with any of the other requirements or obligations of the Regulation, including infringement of the rules on general-purpose AI models.

Supply of incorrect information/failure to supply it to authorities
Up to €7.5m orone per cent of the total worldwide annual turnover of the preceding financial year for the supply of incorrect, incomplete or misleading information to conformity assessment bodies, notifying authorities, or national competent authorities and national competent authorities in reply to a request.

What other EU initiatives are relevant?

On September 28, 2022, the European Commission adopted a proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (EU AI Liability Directive). The Directive aims to harmonise tortious liability rules to make it easier for victims of AI-related damage to claim compensation.

It includes provisions that require Member States to implement rules to require the disclosure of evidence relevant to the alleged harm where AI systems cause damage. There will be a rebuttable presumption of causation where the claimant has shown that the claim is plausible, in which case the provider of the AI system will be deemed to have caused the damage unless it can prove otherwise.

The EU also proposes to modernise the existing rules on the strict liability of manufacturers for defective products through changes to the Product Liability Directive, which covers liability for death or injury and damage to property. The changes would make it:

- Clear that software, AI systems and digital services that are needed to operate a product are covered by the Directive.
- Easier for consumers to claim against manufacturers by requiring manufacturers to disclose evidence, introducing flexibility to the time restrictions to bring claims and by reversing the burden of proof in favour of consumers in cases involving AI.

Does the UK have an equivalent law in the pipeline?

In February 2024, the Department for Science, Innovation and Technology published its response to its consultation, 'A pro-innovation approach to AI regulation'. The UK government proposes to take a different approach to the EU with a non-statutory principles-based framework to be applied by existing sectoral and cross-sectoral regulators. By contrast, the EU AIA will, once finalised, be prescriptive legislation.

The UK's aim is to foster innovation, driving growth and prosperity, while also enabling consumer trust and strengthening the UK's position as "a global leader in AI". The government has confirmed that it believes binding measures will be required in the future for "highly-capable general purpose AI", but that "introducing binding measures too soon, even if highly targeted, could fail to effectively address risks, quickly become out of date, or stifle innovation".

Due to the extraordinary pace of change in the sector, this non-statutory flexible approach is intended to be built up through guidance that can be issued and updated easily.

Central government will coordinate and ensure consistency of approach between regulators by giving guidance on how to apply the principles, including as to the risks posed in particular contexts and what measures should be applied to mitigate them, and by monitoring and evaluating the effectiveness of the framework.

Regulators must provide guidance as to how the principles interact with existing legislation, illustrate what compliance looks like, and produce joint guidance with other regulators where appropriate.

What is the commercial impact of the law(s)?

Businesses will need to establish an inventory of all AI systems used and their risk classifications. They will also need to put in place a comprehensive AI risk-assessment and management programme. This should be put in place alongside guidelines and instructions for the responsible use and, if relevant, development of AI systems, which should address accuracy and safety, fairness and ethical use, explainability, oversight and security issues.

Triggering an AIA category will mean enhancing the rigour and documentation around these processes and tracking to standards approved by the Commission, wherever possible, but the AIA requirements reflect the principles that most regulators would expect to be deployed (perhaps with less rigour) for any substantial AI application. Robust AI governance is necessary to comply with the many existing regulatory obligations that apply to AI, including data protection, competition, employment, and financial services regulation.

Businesses should monitor the progress of the EU AI Liability Directive and the revisions to the EU Product Liability Directive so that they can assess the level of civil liability risk they are potentially taking on when producing or using AI systems.

Data Act

The EU Data Act provides a regulatory framework to govern and make easier the sharing, use and re-use of product-generated data. It also aims to make it easier to switch between cloud providers.

Name of law

EU Data Act: Regulation on harmonised rules on fair access to and use of data. A link to the Council's agreed position (upon which this summary is based) dated March 17, 2023, can be found here.

What is the general purpose of the law?

To facilitate the use of product-generated data by third parties, data interoperability in European data spaces and switching between cloud services providers.

Is the text finalised yet? If not, when do we expect it to be finalised and apply from?

No, it is still going through the EU legislative process. This note is based on the Council's agreed position dated March 17, 2023.

We expect the law to be finalised during the course of 2023. The EU Data Act will enter into force 24 months and 20 days after first publication in the Official Journal of the European Union (**OJEU**).

It is important to note that the Commission will carry out an evaluation of the EU Data Act after two years of its application to assess various aspects of the law, including the categories or types of data to be made accessible and the diminution of charges imposed by data processing service providers for switching, in line with the gradual withdrawal of switching charges.

Who does the law apply to?

Manufacturers of products and suppliers of related services placed on the EU market and the users of such products/services.

Data holders that make data available to data recipients in the EU and those data recipients.

EU public sector bodies where there is an "exceptional need" (e.g. it is necessary to respond to a public emergency).

Data processing services providers who offer data processing services to customers in the EU.

Operators within data spaces and certain vendors using or deploying smart contracts.

What are the main obligations in the law?

As a general point, it is important to note that the obligations and rights under the Data Act are clearly stated to be without prejudice to rights and obligations under applicable data protection law (including the right to establish a lawful basis for data sharing and receipt of the data). The interplay between the rights and obligations under the Data Act and the GDPR is expected to require careful examination.

B2C and B2B IoT data access

Data holders (i.e. the manufacturer/service provider with initial control of the data) must give users (i.e. the owner or renter of the product) readily available free access to the data generated about them.

Before the product is purchased, the data holder must provide various information to the user, including what the data generated will be used for, how the data will be generated, how to access it and the terms of access, information on their identity, means of communication and user rights.

Data users may directly share their data through a data holder or a data intermediary (see Data Governance Act below) with any data recipient (including potential competitors of the relevant data holders) for commercial or non-commercial purposes, such as after-market and value-added services. However, users are prohibited from using the data to develop a product that competes with the product from which the data originates.

Data holders may not share data other than for a purpose of fulfilling the data holder's contractual obligations to the user and are subject to certain obligations on their use of the data. Data recipients are subject to various obligations around the use of the received data and the Data Act includes requirements on the contractual terms governing the data sharing between enterprises.

B2G data access

Data holders must make relevant data available to certain public sector bodies and EU institutions where an exceptional need to use the data is demonstrated. Depending on the circumstances, data holders may be required to provide the data free of charge or may be able to charge.

The public sector body might decide to share the data with national statistical institutes, Eurostat, individuals and organisations carrying out scientific research but must notify the data holder. The data holder has a right to reasonably object to such sharing.

Cloud services switching

Cloud providers will be subject to obligations to help their customers switch to another provider. This includes a right for customers to be able to terminate services on two months' notice (exact period currently being debated), the cloud provider facilitating the porting of data (where the transition must be completed within three months of notice of the intention to switch being given) and removing any switching charges from contracts by a date to be specified (but in not less than three years' time) and gradually reduce such charges in the interim. The relevant rights are to be included in the cloud providers' terms.

Non-personal data, non-EU government access safeguards for cloud service providers

Cloud service providers must put in place GDPR-style reasonable measures (e.g. encryption) to prevent non-EU governmental access to non-personal data that they hold in the EU which would conflict with EU or Member State law (e.g. if the non-EU governmental access would impact on national security or trade secrets without any proportionate consideration of the EU/MS interests) or EU individuals' fundamental rights. Any such access must be based on an international agreement, such as a mutual legal assistance treaty.

Data interoperability

There are provisions that apply to participants of data spaces (which refers to the 9 European Data Spaces). For example, requiring the operators of data spaces to provide APIs with continuous, real-time, machine readable format access to the data and to provide data recipients with the means to enable smart contracts to interoperate within their services/activities.

There are also minimum requirements for smart contracts used for data sharing and the smart contract vendor or organisation deploying it will need to ensure that it provides rigorous access control mechanisms, safe termination of the contract and equivalent levels of protection and confidentiality of trade secrets.

Who will enforce the law?

One or more nominated Member State competent authorities. There will be no new EU coordinating body or procedure for cooperation (other than a simple duty to cooperate with each other) but the European Data Innovation Board (not yet established) will foster exchange of information.

What are the consequences of non-compliance with the law?

There are no new fining powers. Existing authorities will take enforcement action where applicable, e.g. data protection authorities when personal data is involved.

The Data Act gives natural and legal persons the right to lodge complaints with competent authorities.

Non-contractual terms that do not comply with the Data Act will be deemed to be unenforceable. The Data Act does not provide for any other remedies.

Does the UK have an equivalent law in the pipeline?

Not specifically, but Part 3 of the UK Data Protection and Information (No2) Bill (which is subject to further change) sets the ground for regulations analogous to the Data Act.

If yes, how does it compare to the EU law?

The provisions in Part 3 of the Bill enable the Secretary of State to pass regulations which enhance competition between companies by facilitating the sharing of both customer and business data. This follows the existing regulation of Open Banking which successfully boosted competition through enhanced data sharing obligations. It sets the ground for regulations analogous to the Data Act, including: (i) new concepts of customer and business data; and (ii) powers for the Secretary of State or Treasury to make regulations for data holders to provide customer data to customers and requiring data holders to publish business data.

What is the commercial impact of the Data Act?

Data holders that are obliged to make data available to data recipients will need to consider which of the data that they hold is in scope and what transparency is required in this regard.

Businesses providing B2C or B2B data access will need to understand what provisions they should (and are permitted to) include in their data access contracts in order to protect their own IPR.

Cloud service providers will need to repaper existing contracts to meet the new requirements (e.g. by removing switching charges, revising timeframes for switching and termination, and including data availability transparency provisions).

Data Governance Act

The EU Data Governance Act aims to promote sharing and re-use of public sector data and to encourage data altruism. Those wishing to benefit from public sector data for their own analysis (referred to as data users in the DGA) need to understand the conditions for such sharing and re-use.

Name of law

EU Data Governance Act: Regulation (EU) 2022/868 of the European Parliament and of the Council of May 30, 2022, on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (**DGA**). A link to this text can be found here.

What is the general purpose of the law?

The purpose of the DGA is to:

1. Promote the sharing and re-use (for example, for AI or data analytics purposes) of public sector data that are subject to personal data protection, intellectual property or commercial confidentiality rights, and therefore fall outside the 2019 Open Data Directive;
2. Facilitate data sharing across key sectors via common data spaces; and
3. Encourage data altruism.

The DGA sets up a framework on which the Data Act builds, with the Data Act clarifying who can access the data and under what conditions.

Is the text finalised yet? If not, when do we expect it to be finalised and apply from?

Yes. The DGA was adopted on May 30, 2022, and published in the Official Journal of the European Union on June 3, 2022. It entered into force on September 24, 2023.

Who does the law apply to?

The DGA applies to:

i. Public sector bodies (but not state-owned businesses);

ii. Data intermediaries, i.e. neutral third parties who help broker the flow of data from the data source to data users (which may be individuals or companies); and

iii. Recognised data altruism organisations (individuals or companies voluntarily making their data available free of charge so it can be used in the public interest).

What are the main obligations in the law?

Re-use of data held by public sector bodies

The DGA establishes principles and a governance framework around the sharing and re-use of data. This includes:

- A prohibition against exclusive arrangements between public sector bodies and data users – except where providing a service or product in the general interest of the public would not otherwise be possible, and even then for no longer than 12 months;
- Member States have to establish a single information point as an interface for the re-use requests. Public sector bodies must make a decision on each request within two to three months; and
- Public sector bodies must establish and publicise conditions for the re-use of data. The terms for re-use must be non-discriminatory, transparent, proportionate and objectively justified and must not restrict competition.

The DGA is without prejudice to the EU General Data Protection Regulation (**GDPR**). This means that personal data may only be disclosed where a lawful ground for processing has been established under Article 6 of the GDPR (e.g. consent of the individual). Public sector bodies will reserve the right to verify the process, means and results of processing and prohibit the use of the results to preserve data protection where necessary.

Data intermediaries

Data intermediaries must be neutral and cannot themselves use the data which they are facilitating to be re-used. The procedure for data users to access the data intermediary services must be fair, transparent and non-discriminatory.

Other key points about data intermediaries include:

- Data intermediaries will be required to register with a national regulatory body and will appear on a public register;
- Data intermediaries must not provide any other services to avoid conflicts of interest and must be separate legal entities from parts of a business that seeks to exploit the data; and
- Data intermediaries must act in the best interest of data subjects and must provide data subjects with tools to give and withdraw consent.

Data altruism organisations

Individuals and companies may choose to consent to the use of their personal and non-personal data for altruistic purposes. The European Commission must develop a European data altruism consent form. Recognised data altruism organisations will have to be not-for-profit, legally independent and structurally separate. Similar to data intermediaries, data altruism organisations will be required to register with a regulatory body and will appear on a public register.

Data altruism organisations will have a duty to safeguard data subjects' rights and inform them in advance of the altruistic objectives to be achieved and, if applicable, the third country where processing will take place.

They must provide tools for individuals to easily withdraw their consent.

International transfers

The DGA also imposes GDPR style restrictions on transferring non-personal data outside of the EU.

This includes the requirement for data users, data intermediaries and data altruism organisations to take all reasonable measures (including contractual arrangements) to avoid transfers of, or access to, non-personal data held in the EU where this would create a conflict with EU law

or the law of the relevant Member State, unless: (a) an international agreement permits it; or (b) an international judgment directed it, subject to minimum requirements.

Data users will have to notify public sector bodies of their intention to transfer non-personal data to third countries and (with some exceptions, such as where the data has already been anonymised) the data user must, where appropriate with the assistance of the public sector body, inform the legal person whose rights and interests may be affected. The public sector body shall not allow the

re-use of the data unless that legal person gives permission for the transfer. The data user may be required to enter contractual and/or technical arrangements to protect

such non-personal data that is confidential or protected by intellectual property rights. The Commission may adopt model contractual clauses and adopt adequacy decisions to "green light" transfers to certain countries if the Commission is satisfied the data will be afforded appropriate protection.

Who will enforce the law?

The DGA will be enforced by one or more nominated Member State competent authorities. The DPA also introduces the European Data Innovation Board (**EDIB**), an advisory body facilitating cooperation between Member States, creating best practices and helping to ensure consistency.

What are the consequences of non-compliance with the law?

No penalties are specified in the DGA. However, Member States will be able to introduce penalties via national law taking into account recommendations of the EDIB.

Does the UK have an equivalent law in the pipeline?

No, but the UK has similar concerns on data availability so this may serve as a blueprint for the UK.

What is the commercial impact of the law(s)?

There will be greater opportunities to access public sector data and less opportunity for organisations serving the public sector to have exclusive access to data created in the provision of those services.

Organisations wishing to take advantage of the new framework will need to consider how to identify and contract with registered data intermediaries and data altruism organisations appropriately.

Data users may also need to consider the strict conditions of transferring non-personal data obtained via the DGA to third countries. If export of non-personal data is prohibited while export of personal data is permitted, data users will have to make sure not to mix the two, or consider how to comply with requirements in relation to mixed data.

Digital Markets Act

The EU Digital Markets Act (DMA) places obligations on "gatekeepers", including requiring fair and non-discriminatory contractual terms in arrangements with business and consumer users. Organisations need to consider whether they need to file notifications regarding potential gatekeeper designation or whether they might benefit as a business user under obligations imposed on gatekeepers.

Name of law

Digital Markets Act: Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) 2022/1925 (the **DMA**). A link to the text can be found here.

What is the general purpose of the law?

The DMA is an ex-ante instrument with the stated intent of increasing competition and ensuring a level playing field for all digital companies in order to boost innovation and growth and to help smaller companies and start-ups compete with larger players.

It also aims to ensure that consumers have greater choices regarding the services they access.

Is the text finalised yet? If not, when do we expect it to be finalised and apply from?

Yes. The DMA entered into force on November 1, 2022 and the majority of its provisions (there are some limited exceptions) began to apply on May 2, 2023.

Who does the law apply to?

The DMA primarily applies to "gatekeepers" offering "core platform services". Gatekeepers are organisations that: (i) have a significant impact on the internal market (€7.5bn turnover in each of last three financial years or average market capitalisation/fair market value of at least €75bn in last financial year); are an important gateway for business users to reach end users (at least 45 million monthly active EU end users and 10,000 yearly active business users); and (iii) enjoy an entrenched and durable position.

Core platform services include (but are not limited to) search engines, social networking services, video-sharing platform services, app stores, cloud computing services and online advertising services.

What are the main obligations in the law?

The DMA provides rules setting out obligations that apply to gatekeepers (designated in relation to relevant core platform services) include:

- Disclose advertising prices/revenue share information to advertisers and publishers free of charge, on a daily basis;
- Provide advertisers and publishers with free access to advertising performance measurement/verification tools and data;
- Provide anonymised ranking, query, click and view search data to any other third party undertaking providing online search services;
- Allow end users to uninstall preloaded apps;
- Allow hardware providers, business users and alternative service providers effective interoperability with hardware, software and operating systems available to the gatekeeper;
- Provide effective portability of data provided by the end user or generated through the end user's activities;
- Apply fair, transparent and non-discriminatory terms in relation to any product ranking; and
- Provide app developers with fair and non-discriminatory access to app stores, search engines and social networking services.

Examples of prohibitions on gatekeepers (designated in relation to relevant core platform services) include:

- Force business users or end users to use gatekeeper's identification or payment service or web browser;
- Make business users or end users subscribe or register to other core platform services as a condition of using the core platform services;
- Apply obligations that prevent business users from offering the same goods/services to end users on better terms through their own or third party sales channels;
- Engage in self-preferencing in ranking, indexing or crawling;
- Use personal data of users for advertising purposes, unless the user has consented;
- Combine or cross-use personal data across services offered by the gatekeeper unless user has consented; and
- Use non publicly available data generated by business users in their use of the core platform service in competition with the business users.

Other notable provisions include:

- A prohibition on "dark patterns" (i.e. online user interfaces designed to deceive or manipulate the user into a certain choice);
- Where the EU GDPR requires consent for processing personal data, gatekeepers must enable business users to obtain the relevant GDPR-compliant consents from end users; and
- A requirement that gatekeepers report to the Commission to demonstrate how they are complying with their obligations under the DMA.

Who will enforce the law?

National competition authorities will have investigative powers and will be required to report their findings, and provide any requested support, to the Commission. The Commission will be the only regulatory authority with the ability to enforce the DMA.

However, it is widely expected that there will be private enforcement actions by affected business end users.

What are the consequences of non-compliance with the law?

The European Commission can impose fines of up to 10 per cent of a gatekeeper's total worldwide turnover in the previous financial year for non-compliance (or 20 per cent of a gatekeeper's total worldwide turnover for repeat offences). The European Commission can also impose periodic payments of up to five per cent of the average daily worldwide turnover of an undertaking in the previous financial year to assist in compelling it to comply with certain obligations.

In the event of systematic infringements, the European Commission can open a market investigation, potentially leading to additional sanctions. This could include structural remedies such as obliging a gatekeeper to sell a business or parts of it (i.e. selling units, assets, intellectual property rights or brands) or prohibiting a gatekeeper from acquiring any undertaking that provides services in the digital sector.

Does the UK have an equivalent law?

Not yet, but The Digital Markets, Competition and Consumers Bill (the Bill) was introduced into Parliament on April 25, 2023 and is expected to enter into force in 2024. The long-awaited Bill follows the Government's responses to the "reforming competition and consumer policy" and "a new pro-competition regime for digital markets" consultations published in 2022. The legislation will, among other things, underpin and provide statutory powers for the Digital Markets Unit, within the Competition and Markets Authority, which will oversee a new digital regulatory regime, intended to promote greater competition and innovation in digital markets and protect consumers and businesses from unfair practices. The Bill will materially increase regulatory oversight of the digital sector, giving the regulator various powers, including powers to impose new conduct requirements on the largest firms.

What is the commercial impact of the law(s)?

The DMA will have a significant impact on gatekeepers, many of whom will be required to make substantial technical changes as well as amending contractual and policy documentation.

Business users that compete with gatekeepers may benefit from:

- Greater ability to compete with preinstalled apps, as consumers will have a choice to uninstall such apps;
- Interoperability with hardware, software and operating systems provided by gatekeepers;
- Fair product ranking/indexing/crawling services and access to app stores, search engines and social networking services; and
- Gatekeepers being prevented from offering their own services on preferential terms, forcing use of identification, payment processing or web browsing services, or making access to particular core platform services contingent on subscription/registration to other services.

Users of services provided by gatekeepers will likely benefit from:

- Increased transparency in terms of pricing and product/audience metrics; and
- The ability to obtain any consent required under GDPR via the gatekeepers' service.

End users can expect to have more choice, as smaller providers will have more freedom and incentive to innovate or provide customised services alongside gatekeeper offerings.

Digital Services Act

The Digital Services Act (DSA) places obligations on all digital services that connect consumers to goods, services and content, including "intermediaries" that provide conduit, caching and hosting services. And there are new procedures for the removal of illegal content. The UK Online Safety Act also contains some similar provisions. Companies need to consider if they are subject to these enhanced obligations and devise a strategy on how to comply.

Name of law

Digital Services Act, Regulation on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC (**DSA**). A link to the text can be found here.

What is the general purpose of the law?

The stated purpose of the DSA is to modernise the existing e-commerce Directive and address illegal content, in transparent advertising and disinformation. It imposes obligations on all digital services that connect consumers to goods, services and content including intermediaries that provide conduit, caching and hosting services. EU Member States have traditionally adopted their own methods for addressing illegal content but the DSA intends to harmonise these approaches at EU level.

Is the text finalised yet? If not, when do we expect it to be finalised and apply from?

Yes, the DSA entered into force on November 16, 2022, and will apply (for the most part) from February 17, 2024. However, obligations on very large online platforms and very large online search engines applied from February 17, 2023. In addition, all providers of online platforms and online search engines were required to publicise details of the number of average monthly active users from February 17, 2023 (and at least every six months thereafter).

Who does the law apply to?

The DSA applies in a funnel-like manner with certain obligations applying to all intermediary services providers (**ISPs**) while certain other obligations relate only to specific intermediary services that are provided by larger suppliers.

The DSA has extra territorial application, such that it will apply to non-EU organisations that target the EU market, requiring such non-EU organisations to designate a legal representative in an EU Member States where the ISP offers its services.

The categories of services and platforms referred to in the DSA are:

Intermediary service providers being providers of:

"Mere conduit" services
These are services consisting of the transmission of information provided by a service recipient in a communication network, or the provision of access to a communication network (e.g. virtual private networks, domain name system services, internet exchange points, etc.).

"Caching" services
These are services involving the automatic, intermediate and temporary storage of information provided by a service recipient for the purposes of making the onward transmission of that information to other recipients more efficient (e.g. content delivery networks).

"Hosting" services
These are services that store information provided by a service recipient (e.g. cloud services).

Online platforms

Services that, at the request of the recipient of the service, store and disseminate information to the public, e.g. online marketplaces, app stores, collaborative economy platforms and social media platforms.

As set out below, additional obligations are imposed on online platforms that have 45 million or more average monthly active users in the EU and which are designated as "very large online platforms" by the Commission.

Online search engines

Services that allow users to input queries in order to perform searches of websites and which return results in a format in which information related to the requested content can be found. Additional obligations apply to "very large" search engines, which is based on the same criteria as "very large" online platforms.

What are the main obligations in the law?

All intermediary service providers

ISPs must comply with orders from the relevant national authorities to act in relation to illegal content. However, the DSA confirms that ISPs have no general obligation to monitor content and are generally exempt from liability even where they voluntarily take steps to detect, identify or remove illegal content or take measures necessary to comply with national or EU law. However, ISPs must provide certain information to authorities about the actions they have taken in relation to illegal content. ISPs must appoint a single point of contact for Member State and European-wide authorities and a single point of contact for recipients of the services. Details of the single point of contact must be made public.

ISPs must prepare publicly available reports on their content removal and moderation activities on an annual basis.

ISPs must include information on any restrictions regarding the information provided by users in connection with the service in their terms and conditions. The required information includes details of the content moderation mechanisms applied, algorithmic decision-making and human review. The information must be provided in clear and unambiguous language and, where applicable, presented in a way minors can understand. ISPs must inform recipients of significant changes to their terms and conditions.

Hosting services (including providers of online platforms)

Hosting service providers must implement a mechanism to allow third parties to report alleged illegal content by electronic means and in a user-friendly manner.

They must also provide recipients of the service with a statement regarding decisions taken to remove content and/or suspend or terminate recipients' accounts (where the relevant electronic contact details of the recipient are known). Such statements of reasons must contain certain at a minimum the information set out in the DSA, including information about the use of automated means in taking the decision, its alleged illegality and the available redress and complaint-handling mechanisms.

Where a hosting service provider becomes aware of information giving rise to a suspicion that a criminal offence involving a threat to the life or safety of a person is (or will) take place, it must inform the law enforcement or judicial authorities of the Member State(s) concerned promptly of its suspicion and provide all available information.

Online platforms

Obligations imposed on online platforms (excluding micro or small enterprises) include requirements to:

- Provide internal complaint handling systems to enable users to challenge platforms' decisions to remove content and inform users of their ability to refer disputes to an out-of-court dispute settlement body;
- Publish detailed reports on their activities relating to the removal and the disabling of illegal content or content contrary to their terms and conditions (this goes further than the general obligations for ISPs);
- Put in place appropriate and proportionate measures to ensure a high level of privacy, safety and security of minors on their service;
- Online marketplaces must collect certain information from traders to verify their reliability and suspend traders that that do not provide this information within 12 months; and
- Ensure that their online interfaces are designed and organised to enables traders to comply with their obligations regarding pre-contractual information, compliance and product safety information.

There are increased obligations on transparency:

- In relation to online advertising, users must be provided with clear information in real time so they can identify: (i) that they are seeing advertisements; (ii) on whose behalf advertisements are presented or paid for; and (iii) meaningful information that must be directly and easily accessible from advertisements about the main parameters used to target specific users;
- Recommender systems (i.e. an automated suggestion system to promote specific content) must publish information about how their systems works, including the criteria for determining what information is displayed; and
- All providers of online services must report numbers of active users and information about disputes with, and suspension of the accounts of, service recipients.

The DSA expressly prohibits online platform providers from using "dark patterns" (i.e. deceptive interfaces that trick users into doing things, like agreeing to hidden costs, disguised ads, etc.) and sets out rules for how online platform providers that allow contracts to be concluded online should present certain information.

VLOPs and VLOSEs

These very large providers are subject to additional obligations including requirements to conduct an annual risk assessment to adopt and document effective mitigation measures. They must also establish an independent compliance function comprised of one or more appropriately knowledgeable and qualified compliance officer(s), including a dedicated head of compliance function who reports directly into the management body of the VLOP or VLOSE.

VLOPs and VLOSEs are also subject to additional transparency obligations including in relation to the use of online advertising and recommendation systems.

VLOPs and VLOSEs will also be required to pay annual supervisory fees which shall not exceed 0.05 per cent of worldwide annual net income in the preceding financial year.

Who will enforce the law?

Each Member State will designate a competent authority as its Digital Services Coordinator, with powers to investigate compliance with the DSA, seek information from ISPs and take enforcement action.

The DSA provides for a formal coordination and escalation process and a dispute resolution regime between Member States and the Commission to ensure

consistency in relation to enforcement. This has similarities to the equivalent mechanism in the EU General Data Protection Regulation.

The DSA provides for enhanced supervision of VLOPs and VLOSEs, and the Commission is entitled to initiate proceedings against these organisations in certain circumstances. Digital Service Coordinators may also request that the Commission assess suspected infringements by VLOPs and VLOSEs.

A European Board for Digital Services made up of the Member State Digital Services Coordinators will be set up to provide support and advice to the Commission and Member State authorities. The Board will also issue opinions, recommendations and advice to the Digital Service Coordinators, support and promote the development of European standards and codes of conduct, and help coordinate joint investigations.

What are the consequences of non-compliance with the law?

Member States will be required to adopt rules on penalties which must be "effective, proportionate and dissuasive". Fines may be up to six per cent of global turnover in the preceding financial year of the infringing party. Member States shall ensure that the maximum amount of the fine that may be imposed for the supply of incorrect, incomplete or misleading information, failure to reply or rectify incorrect, incomplete or misleading information and failure to submit to an inspection shall be one per cent of annual global turnover in the preceding financial year Member States are also entitled to impose periodic penalties of up to five per cent of the average worldwide turnover of the ISP in the preceding financial year.

Recipients of the service must have the right to seek compensation from ISPs for any loss or damage resulting from infringement of the ISPs' DSA obligations.

The Commission has similar fining powers in relation to non-compliance by VLOPs or VLOSEs, and can require VLOPs or VLOSEs to develop action plans to deal with non-compliance.

Does the UK have an equivalent law in the pipeline?

Yes. There are some provisions of the Online Safety Act that are similar to aspects of the DSA concerning duties on restricting illegal content, updating terms and conditions and implementing reporting mechanisms. However, the Online Safety Act has no equivalent to the prohibition on imposing general monitoring obligations in the DSA, nor does it mirror the DSA's exemptions from liability for illegal content on their platforms. Service providers are required to take proportionate measures to prevent all users from encountering certain types of illegal content and children from encountering certain types of harmful content.

What is the commercial impact of the DSA?

Whilst some of the obligations under the DSA are only applicable to the very largest platforms, many of the obligations in the DSA will apply to a large number of organisations because of the broad definition of "intermediary services". Organisations will need to carefully consider whether they are ISPs and, if so, whether they provide the services attracting enhanced obligations.

Organisations will need to address the practical impact of obligations to appoint legal representatives, points of contact and compliance officers. But they will also need to carefully consider how to comply with enhanced transparency obligations and the requirements to publish certain user-facing and regulator-facing notices in relation to recommender systems and online advertising. It is currently unclear how the required information will be presented and what level of detail will be given, but ISPs will need to be prepared to make technical changes to their platforms to comply with their obligations.

More generally, content moderation obligations, dealing with illegal content and assessment traders will require organisations to make changes to their practices and technical changes to their system. These will take time and organisations will need help to understand precisely what obligations under the DSA apply in short order and what exactly they need to do.

NIS2

Both the EU and the UK are amending their laws around Network and Information Security to strengthen security against cyber-risks in an increased range of sectors. Impacted organisations need to understand what new measures they may need to put in place to comply with the changes.

Name of law

The Network and Information Systems Directive (EU) 2022/2555 of the European Parliament and of the Council of December 14, 2022, on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing and replacing Directive (EU) 2016/1148 (**NIS2**). A link to this text can be found here.

What is the general purpose of the law?

NIS2 was introduced following increased digitisation and malicious cyber activity globally and its stated aim is to overcome the shortcomings of the previous Cybersecurity Directive ((EU) 2016/1148) (NIS1). The European Commission identified various deficiencies in N151, including limited scope, lack of harmonisation across Member States, inconsistent levels of cyber resilience across Member States and business sectors, and a lack of joint crisis response mechanism. NIS2 widens and strengthens the cybersecurity and incident notification requirements under NIS1, and introduces new measures aimed at managing cyber risk across the EU to prevent unauthorised access and use of IT systems – namely, it imposes cyber risk management, incident reporting and information-sharing obligations on certain types of organisations. It also broadens the types of organisations operating or established in the EU subject to these requirements.

Is the text finalised yet? If not, when do we expect it to be finalised and apply from?

Yes. On November 28, 2022, the European Council adopted NIS2. Member States must adopt and publish the measures necessary to comply with NIS2 by October 17, 2024. Those measures shall apply from October 18, 2024, after which NIS1 will be repealed.

Who does the law apply to?

NIS2 broadens the sectors required to comply. Under NIS1 (which is in force in the UK), obligations are placed on "operators of essential services" (**OESs**) (e.g. banks, healthcare providers, energy companies, etc.) and relevant "digital service providers" (**DSPs**) (e.g. cloud providers, online market places, search engines, etc.). However, under NIS2, this list will expand to include postal and courier services, data centre services, waste water and waste management and manufactures of certain critical services such as pharmaceuticals, medical devices and chemicals.

NIS2 also removes the distinction between OESs and DSPs, which the Commission considered obsolete on the basis that it does not reflect the actual importance of the sectors or services for the societal and economic activities in the internal market. NIS2 now classifies in-scope entities based on their importance (i.e. depending on the sector they operate in) and divides them into "essential entities" and "important entities" as detailed in Annexes I and II. For NIS2 to bite, entities must provide their services or carry out their activities in the EU and be either an "essential" or an "important" entity active in a specified sector.

What are the main obligations in the law?

Incident reporting

Under NIS2 there will be a three-stage process for reporting security incidents to the relevant authorities. An "early warning report" must be submitted within 24 hours. Next, a fuller "incident notification" should be submitted within 72 hours. A "final report" should be submitted within one month. This final report should provide a detailed description of the incident, including its severity and impact and the mitigating measures that have been taken.

NIS1 provides an expansive list of factors that OESs and DSPs must consider to determine whether an incident must be reported. But this has led to over-reporting of incidents, which NIS2 seeks to address. Under NIS2, an in-scope entity must report only incidents which: (i) cause, or have the potential to cause, severe operational disruption of the services or financial losses for the entity concerned; or (ii) have affected, or are capable of affecting, other natural or legal persons by causing considerable material or non-material damage.

Registration

Under NIS2, certain entities (including cloud providers and data centres) will need to submit a registration to the European Union Agency for Cyber Security (**ENISA**). The information for registration includes the relevant entity's name, sector, address, up-to-date contact details, the Member States where the entity provides its services and the entity's IP ranges.

Cyber-security risk management measures

NIS1 imposes obligations to implement technical and organisational measures to manage security risks of systems of facilities. NIS2 expands upon these requirements with a long list of the types of measures that should implemented as a minimum. It is described as an "all-hazards approach". Measures include ensuring basic cyber hygiene practices and cybersecurity training, cryptography and encryption, multi factor authentication or continuous authentication solutions, and supply chain security.

This means that businesses that are not directly caught by NIS2 could be indirectly impacted, because in-scope entities are encouraged to incorporate cybersecurity risk management measures into their contractual arrangements with their supply chains.

Obligations on "management bodies"

NIS2 imposes new obligations on "management bodies". They must: (i) have regular training and must offer similar training to their employees; and (ii) oversee the implementation of the cyber-security risk management measures described above.

Essential entities must appoint a natural person who is responsible for the compliance of (or is acting as a legal representative of) an essential entity – this person must have the power to ensure compliance with NIS2 and can be liable for breach of their duties to ensure compliance.

Who will enforce the law?

NIS2 requires Member States to designate one or more "competent authorities" responsible for cybersecurity and certain supervisory tasks that will have broader and stronger powers to supervise and sanction in-scope entities than under NIS1. These powers can apply differently depending on whether an entity is considered essential or important.

NIS2 also sets out a regulatory framework to facilitate co-operation with regards to enforcement and introduces the following new initiatives:

- In addition to the role of the Computer Security Incident Response Team (**CSIRT**) and CSIRT network established under NIS1, NIS2 will create the European Cyber Crises Liaison Organisation Network (**EU-CyCLONe**), for the co-ordinated management of large-scale cybersecurity incidents and to ensure regular exchange of information amongst Member States and EU bodies;
- ENISA will be responsible for developing and maintaining a European vulnerability registry to enable entities, and suppliers of network and information systems, to document vulnerabilities. Entities will be encouraged to invite "ethical hackers" to examine their systems and identify vulnerabilities;
- An EU-level reporting and peer review system will be created (and facilitated by Member States) so that in-scope entities (and third party suppliers which need to meet the security standards of in-scope entities whose supply chains they are part of) can voluntarily exchange cybersecurity information in relation to, for example, cyber threats, near misses, and adversarial tactics; and
- Member States, cooperating with the Commission and ENISA, will have powers to carry out risk assessments of critical EU-level ICT supply chains.

What are the consequences of non-compliance with the law?

Under NIS2, essential entities will be subject to a complete, ex ante, supervisory regime. National authorities will have core powers to supervise these entities, including the ability to carry out on and off-site inspections, random checks, regular and ad hoc audits, and security scans to check for vulnerabilities. National authorities will also be able to request certain information and evidence of compliance. Important entities will be subject to lighter, ex post, supervision in the event of evidence or indications of non-compliance.

Where non-compliance is confirmed, competent authorities can exercise enforcement powers that include the power to order entities to publicise aspects of the infringement, to cease certain conduct or to implement recommendations. In regard to important entities, competent authorities will not have the power to temporarily suspend certifications or authorisations or to temporarily ban CEO or GC level representatives from discharging managerial responsibilities – these sanctions can only be imposed on essential entities.

NIS2 also distinguishes between essential and important entities in relation to administrative fines. For essential entities, the maximum fine set by Member States must be at least €10m or two per cent of their total worldwide annual turnover of the preceding financial year, whichever is higher. For important entities, the maximum fine must be at least €7m or at least 1.4 per cent of their total worldwide annual turnover of the preceding financial year, whichever is higher.

Does the UK have an equivalent law in the pipeline?

The UK implemented NIS1 prior to Brexit. The UK will not implement NIS2 but is working on its own proposals to amend the NIS regime. For example, expanding the scope of digital service providers to bring "managed services" in scope, and, also, expanding the current incident reporting duties to include incidents that do not actually affect the continuity of the service directly, but nonetheless pose a significant risk to the security and resilience of the entities in question and the essential services they provide.

What is the commercial impact of the NIS2?

Organisations will need to consider whether or not they are caught by the NIS2 requirements. Whilst this will generally be obvious, in some cases a more detailed analysis of the law's application may be needed.

In-scope organisations must plan, and budget, for these changes. The EU impact assessment on NIS2 suggested that in-scope companies *"would need an increase of maximum 22 per cent of their current ICT security spending for the first years following the introduction of the new NIS framework (this would be 12 per cent for companies already under the scope of the current NIS Directive)".*

Policies and procedures must also be reviewed to check they meet the new requirements. This will be particularly important in relation to a breach notification where three different reports will need to be submitted.

NIS2 provides that in-scope entities must guarantee the security of ICT supply chains – i.e. they must require third parties to meet their security standards (impacting businesses outside the scope of NIS2). When considering whether the security of the supply chain of services is appropriate, in-scope entities must also take into account the vulnerabilities of each specific supplier and the overall quality of products and cybersecurity practices of their suppliers.

Key contacts

Marcus Evans
EMEA Head of Information governance, privacy and cybersecurity
Tel +44 20 7444 3959
marcus.evans@nortonrosefulbright.com

Jurriaan Jansen
Partner
Tel +31 20 462 9381
jurriaan.jansen@nortonrosefulbright.com

Nadège Martin
Partner
Tel +33 1 56 59 53 74
nadege.martin@nortonrosefulbright.com

Christoph Ritzer
Partner
Tel +49 69 505096 241
christop.ritzer@nortonrosefulbright.com

Lara White
Partner
Tel +44 20 7444 5158
lara.white@nortonrosefulbright.com

Miranda Cole
Partner
Tel +44 20 7283 6000
miranda.cole@nortonrosefulbright.com

Our global offices

Our office locations

7000+
People worldwide

3000+
Legal staff worldwide

50+
Offices

Key industry strengths

- Financial institutions
- Energy, infrastructure and resources
- Transport
- Technology
- Life sciences and healthcare
- Consumer markets

Europe

- Amsterdam
- Athens
- Brussels
- Düsseldorf
- Frankfurt
- Hamburg
- Istanbul
- London
- Luxembourg
- Milan
- Munich
- Paris
- Piraeus
- Warsaw

United States

- Austin
- Chicago
- Dallas
- Denver
- Houston
- Los Angeles
- Minneapolis
- New York
- St Louis
- San Antonio
- San Francisco
- Washington DC

Canada

- Calgary
- Montréal
- Ottawa
- Québec
- Toronto
- Vancouver

Latin America

- Mexico City
- São Paulo

Asia Pacific

- Bangkok
- Beijing
- Brisbane
- Canberra
- Hong Kong
- Jakarta[1]
- Melbourne
- Perth
- Shanghai
- Singapore
- Sydney
- Tokyo

Africa

- Bujumbura[3]
- Cape Town
- Casablanca
- Durban
- Harare[3]
- Johannesburg
- Kampala[3]
- Nairobi[3]

Middle East

- Dubai
- Riyadh[2]

1 TNB & Partners in association with Norton Rose Fulbright Australia

2 The Company of Mohammed A. Altammami for Legal Services in association with Norton Rose Fulbright LLP

3 Alliances

NORTON ROSE FULBRIGHT

Norton Rose Fulbright provides a full scope of legal services to the world's preeminent corporations and financial institutions. The global law firm has more than 3,000 lawyers advising clients across more than 50 locations worldwide, including Houston, New York, London, Toronto, Mexico City, Hong Kong, Sydney and Johannesburg, covering the United States, Europe, Canada, Latin America, Asia, Australia, Africa and the Middle East.

Law around the world

nortonrosefulbright.com

0193839_EMEA – 05/24