STEPHENSON HARWOOD

Digital Decade

Horizon scanning upcoming digital regulation

January 2023

#techintelligence

Digital Decade: an overview of upcoming digital legislation

In March 2021, the European Commission presented its vision for Europe's digital transformation by 2030. As part of that vision, the Commission proposed to introduce a raft of new legislation which is expected to come into force within the next few years – the EU's **Digital Decade**. Alongside this, the UK government is preparing to carve its own way for digital regulation, with a focus on "**driving growth and unlocking innovation**".

These legislative proposals will introduce new rules in areas such as data, AI and cybersecurity and impose new obligations on Big Tech companies. However, with diverging approaches from Brussels and the UK, businesses will need to consider which rules apply to them and the steps which need to be taken to ensure compliance.

In this insight we provide a summary of the key legislative proposals.

Simon Bollans
Partner, Technology

T: +44 20 7809 2668
E: simon.bollans@shlegal.com

Katie Hewson
Partner, Data Protection

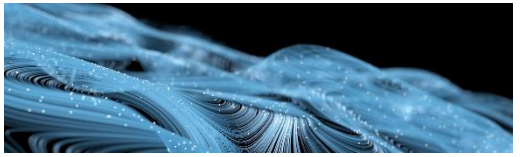
T: +44 20 7809 2374
E: kate.hewson@shlegal.com

"The scope of the regulatory changes over the next few years, both in the UK and EU, is significant and will have an impact most, if not all, business. Time is of the essence for clients to understand how these changes will impact their operations." Simon Bollans, partner and head of Stephenson Harwood's Technology Sector Group

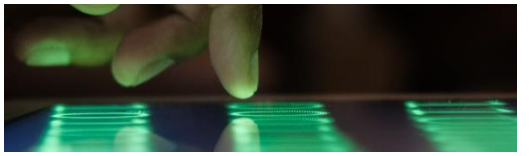
Key themes:

Regulating the tech giants

Data governance and usage



Artificial intelligence



Cyber security

The Legal 500 United Kingdom Leading Firm 2023

Chambers Ranked in UK 2023

Stephenson Harwood LLP

Regulating online "gatekeepers" and protecting against online harms

***"The DMA will change the digital landscape profoundly"* – Margrethe Vestager**

(Executive Vice President, European Commission for A Europe Fit for the Digital Age)

Digital Markets Act ("DMA")

The DMA is set to regulate the main services provided by the biggest online platforms operating in the EU covering the likes of Google, Apple, Amazon and Microsoft.

Who will the DMA apply to?

Applies to companies that (i) provide core platform services most prone to unfair business practices; (ii) meet certain market capitalisation/annual turnover thresholds; and (iii) have a vast reach to users across the EU. Any in scope companies will be known as the "Gatekeepers."

Key provisions

Obligations and prohibitions will be placed on the gatekeepers in their daily operations to ensure fair and open digital markets including:

- Giving businesses access to data generated through their use of Big Tech platforms.
- Allowing businesses to conclude contracts with customers acquired through Big Tech platforms on third-party platforms.
- Making platforms interoperable with smaller platforms. For example, WhatsApp and Facebook Messenger will have to work with smaller messaging platforms if requested.

Penalties

Fines of up to 10% of a gatekeeper's global turnover for non-compliance (which may increase to 20% if a gatekeeper commits a second violation in less than eight years following the first).

Current status

Entered into force on 1 November 2022.

Gatekeeper notification and review process will start from 2 May 2022 (with a 3 July 2023 deadline). Once designated, gatekeepers will have six months to comply with the DMA's requirements.

Regulating online "gatekeepers" and protecting against online harms

***"These new rules launch us into a new age, where big online platforms will no longer behave like they are too big to care*" - Thierry Breton**

(Commissioner for Internal Market)

Digital Services Act ("DSA")

The DSA is set to regulate how online platforms with EU users handle illegal or potentially harmful online content by establishing a powerful transparency and accountability framework.

Who will the DSA apply to?

Companies caught by the DSA will include intermediary services, hosting services and online platforms. The obligations placed on different online companies will be proportionate to their role, size and impact in the online ecosystem.

Key provisions

- Obligations to identify and remove illegal content, transparency obligations on steps taken to combat illegal information and transparency requirements in relation to online advertisements.
- Special protection measures needed where platforms are accessible by minors, to ensure their online safety.
- A ban on the use of dark patterns and on targeting advertising at minors using their personal data.

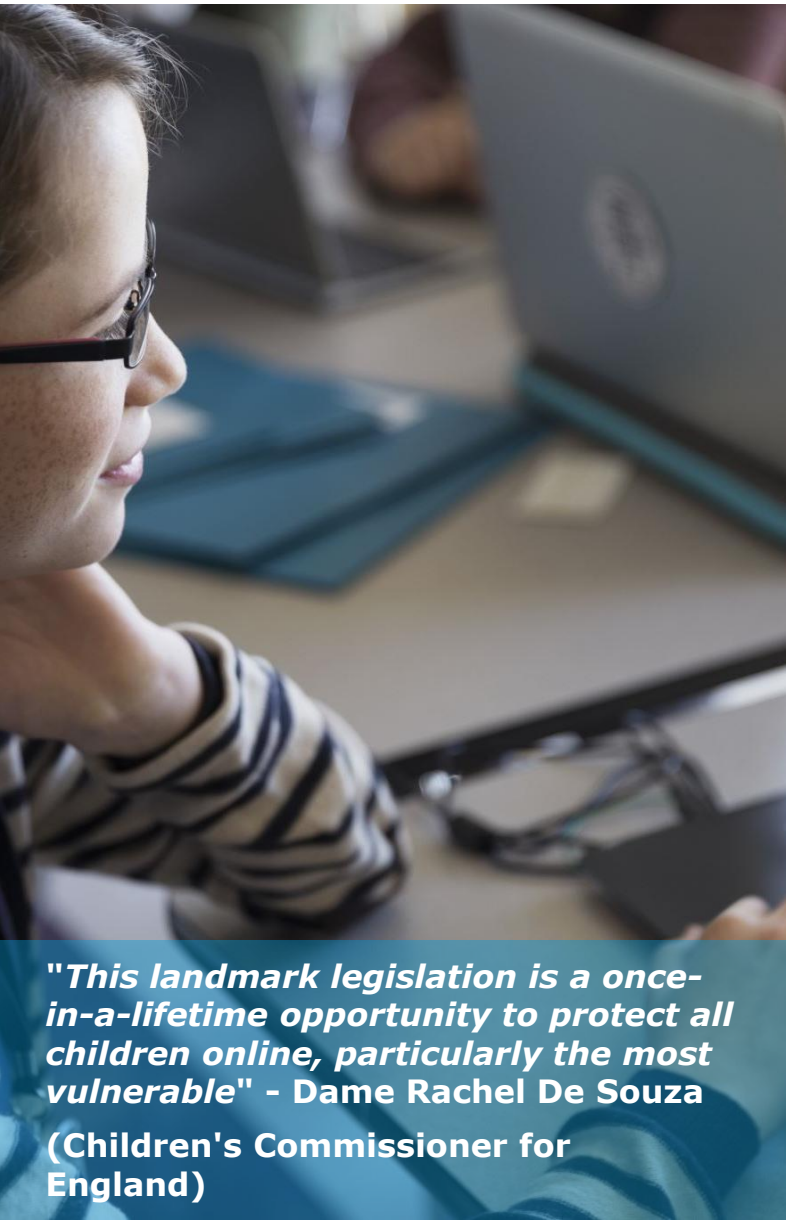
Penalties

Fines of up to 6% of annual global income/turnover on platforms and search engines that fail to comply.

Current status

Came into force on 16 November 2022 and will apply from 17 February 2024 following a 15-month lead-in period.

Regulating online "gatekeepers" and protecting against online harms



***"This landmark legislation is a once-in-a-lifetime opportunity to protect all children online, particularly the most vulnerable*" - Dame Rachel De Souza**

(Children's Commissioner for England)

UK Online Safety Bill ("OSB")

Brexit has led to the UK taking a parallel approach to the Digital Services Act, in the form of the OSB. This seeks to regulate certain online services and to tackle illegal and harmful online content.

Who will the OSB apply to?

The current draft requires companies whose services are accessible to UK users to protect those users from illegal and some "legal but harmful" material.

Key proposals

- Platforms targeted at children will have a duty to protect them from harmful material.
- Some large, high-risk platforms will be required to provide control to users over what content they see so that legal but harmful material can be hidden if desired, as well as setting out what content is acceptable or not acceptable in their terms and conditions.
- Rather than being enforced centrally, the OSB would place enforcement obligations on the online service providers themselves.

Penalties

Potential fines for non-compliance could be as great as £18 million or 10% of annual global turnover.

Current status

The OSB is awaiting its second reading in the House of Lords and is not likely to pass into law until Summer 2023.

Data governance and usage

EU Data Act ("DA")

The DA is set to introduce new rules on who can use and access data generated in the EU across all economic sectors. The intention is to unlock the value and benefits in data by facilitating broader uses and sharing of data. It will cover all types of digital data, both personal and non-personal.

The GDPR will continue to apply alongside it, where any personal data is involved.

Who will the DA apply to?

Will apply to (i) manufacturers and providers of connected products; (ii) businesses that make their data available to recipients in the EU; (iii) data processing services with customers in the EU; and (iv) public sector bodies in the EU. Some SMEs and micro-enterprises will be exempt from the DA.

Key proposals

- Manufacturers and service providers of connected products will need to make the data generated by such products accessible to end users on request.
- Data holders will have to make data available to public bodies in the EU without undue delay where there is an exceptional need to use the requested data.
- Non-personal data held in the EU by data processing services must not be accessed by non-EU governmental entities or transferred internationally.

Penalties

The current proposals do not currently include any GDPR-style penalties, but states that infringements will be sanctioned by "effective, proportionate, and dissuasive fines".

Current status

The final text of the DA is unlikely to be finalised until the second quarter of 2023 and could be further delayed by the trilogue negotiations.

***"Data must be processed according to European values if we aim to shape a safer digital future."* Wojciech Wiewiórowski**

(European Data Protection Supervisor)

Data governance and usage

EU Data Governance Act ("DGA")

The DGA aims to boost data sharing in the EU, by giving start-ups and other businesses better access to big data, which they can use to develop new products and services.

Who will the DGA apply to?

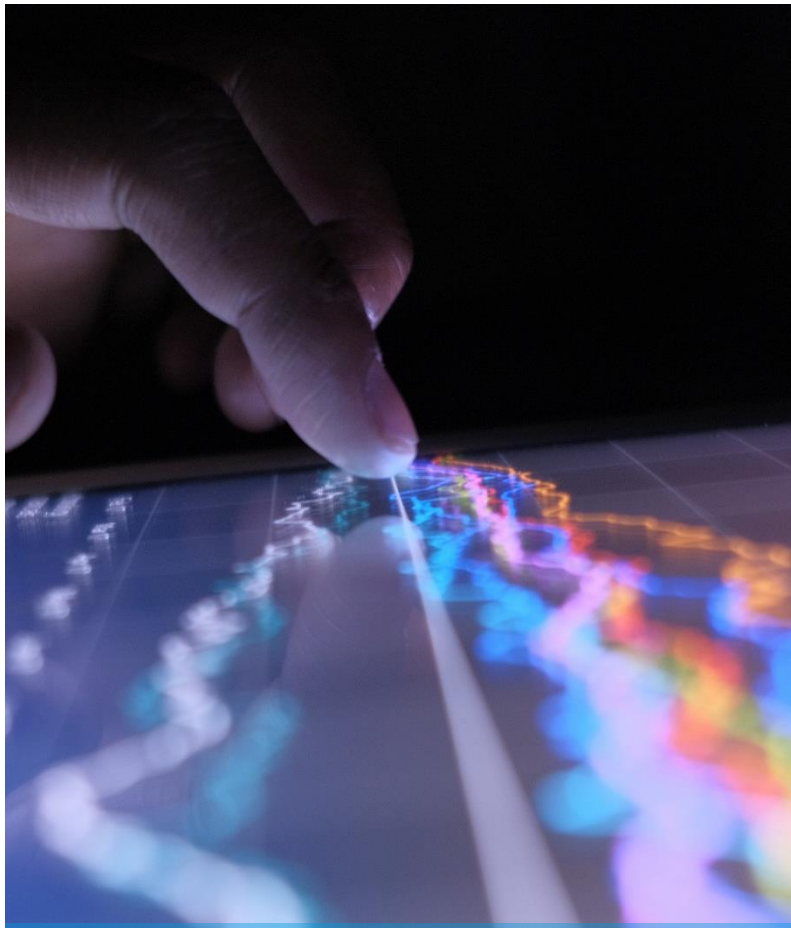
The DGA will regulate how public sector bodies share DGA data, as well as the intermediaries that facilitate data sharing. Data governed by the DGA will include both personal and non-personal data.

Key provisions

- Public sector bodies will be encouraged to share data through "European data spaces", and new rules will make it easier for organisations and individuals to share data for the benefit of society.
- Public bodies will be restricted in their ability to grant exclusive arrangements for sharing DGA data.
- Restrictions on transfers of DGA data to outside of Europe (with a similar adequacy regime for DGA data to that under the GDPR).
- A new business model for data intermediary services (e.g. a data hosting marketplace for the sharing of data), with such intermediaries requiring a licence to carry out their services.
- Member States will be required to establish supervisory authorities to act as information points, providing assistance to government bodies.

Current status

Came into force on 23 June 2022. Following a 15 month lead-in period, the DGA will apply from 24 September 2023.



***"Our goal with the DGA is to set the foundation for a data economy in which people and businesses can trust"* - Angelika Niebler**

(Lead MEP)

Data governance and usage

ePrivacy Regulation ("ePR")

The ePR is set to replace the ePrivacy Directive. The ePR will regulate various areas of electronic privacy, mostly in relation to electronic communications within the EU. The GDPR's general rules on personal data will compliment the ePR's specific rules on electronic communications.

Who will the ePR apply to?

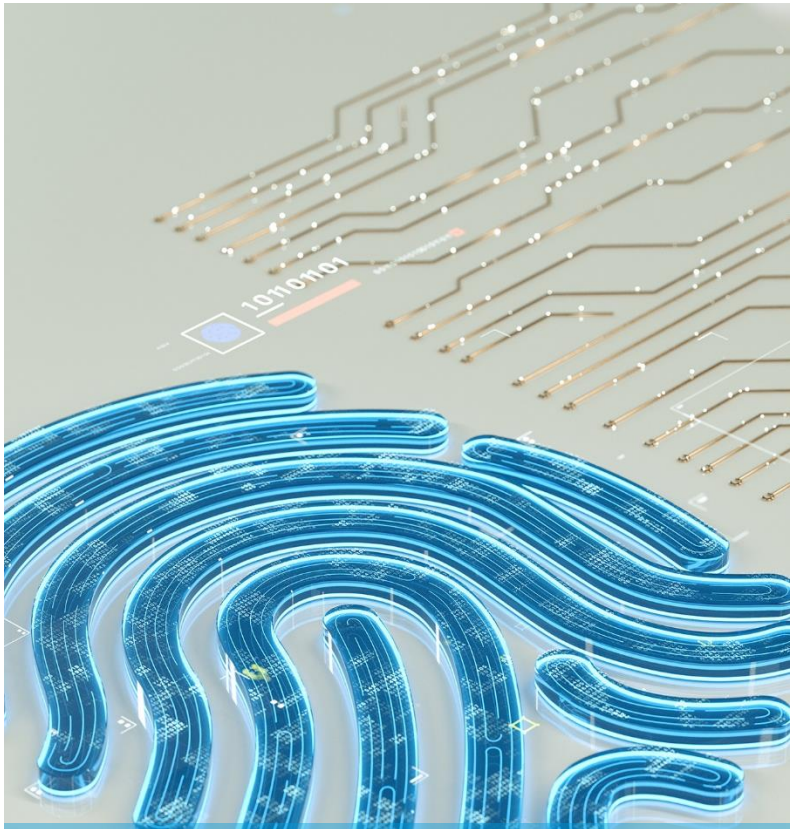
As with the ePrivacy Directive, not only will the ePR apply to personal data used in electronic communications, but also to certain other non-personal communications data.

Key proposals

- Widening the privacy rules on electronic communications to apply to new players such as WhatsApp and Facebook Messenger. This is to ensure that these services guarantee the same level of privacy protection over electronic communications as traditional telecoms providers which are already regulated.
- Simplifying requirements for the usage of cookies and similar technologies.
- Banning unsolicited electronic communications by email, text and automated calling machines. Includes new protections such as requiring marketing callers to display their phone number or use a special prefix to indicate that it is a marketing call.
- Enhancing privacy requirements for content generated from electronic comms and metadata. Once received, all content will need to be deleted, anonymised or processed in accordance with the GDPR. All metadata will need to be deleted or anonymised once no longer needed for billing.

Current status

The final text is yet to be agreed as the European Parliament and the Council still disagree on a number of issues. The ePR is unlikely to enter into force soon, but there may well be further developments in 2023.



"We now have a mandate that strikes a good balance between solid protection of the private life of individuals and fostering the development of new technologies and innovation" **- Pedro Nuno Santos**

(Portuguese Minister for Infrastructure and Housing, President of the Council)

Data governance and usage

UK Data Protection and Digital Information Bill ("Bill")

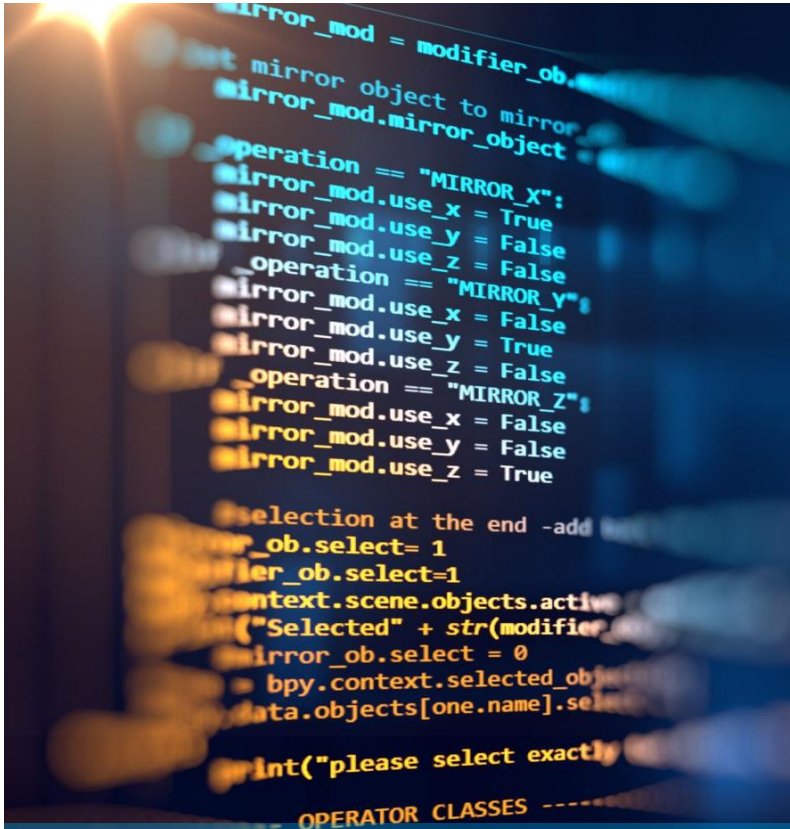
The Bill aims to update and simplify the UK's data protection framework by making extensive amendments to (i) the UK GDPR; (ii) the UK Data Protection Act 2018; and (iii) the UK Privacy and Electronic Communications Regulations. The UK government hopes the Bill will reduce compliance burdens on organisations, while still maintaining high standards.

Key proposals

- Clarifying that an individual should only be considered "identifiable" if (i) a controller; (ii) a processor; or (iii) others who are reasonably likely to receive the information, are reasonably likely to be able to identify the individual.
- Introducing a list of "recognised" legitimate interests that do not require the completion of a legitimate interests assessment.
- Replacing the "manifestly unfounded or excessive" threshold for refusing data subject access requests ("DSARs") under the UK GDPR to "vexatious or excessive" in order to reduce the burden of DSARs on businesses.
- Loosening the restriction on automated decision-making to primarily focus on the use of special category data in automated decisions.
- Introducing broad consents for processing data for scientific research purposes and clarifying that the definition of scientific research includes privately-funded research.

Current status

The second reading of the Bill was scheduled for 5 September 2022, however it was postponed due to the changes in UK government, and a new date is yet to be set. We anticipate that it will move ahead this year.



"Our new Data Reform Bill will make it easier for businesses and researchers to unlock the power of data to grow the economy and improve society, but retains our global gold standard for data protection" **- Nadine Dorries**

(Former Minister for Digital, Culture, Media and Sport)

Regulating the use of Artificial Intelligence

"On Artificial Intelligence, trust is a must, not a nice to have. With these landmark rules, the EU is spearheading the development of new global norms to make sure AI can be trusted" **- Margrethe Vestager**

(Executive Vice President, European Commission for A Europe Fit for the Digital Age)

EU Artificial Intelligence Act ("AI Act")

The EU is proposing to introduce legislation that will address fundamental rights and safety risks specific to AI systems.

Who will the AI Act apply to?

The AI Act will apply if the impact of the AI system occurs in the EU, regardless of the location of the provider or the user.

Key proposals

- Will introduce a four-tiered risk framework being "minimal or no risk," "limited risk," "high risk," and "unacceptable risk". Each tier will be governed by proportionate rules for providers and users of AI systems.
- Banning certain unacceptable risk AI practices, such as certain social scoring and real-time facial recognition by law enforcement in public spaces.
- Requiring providers of high-risk AI systems to take extra steps, such as (i) implementing risk and quality management systems; and (ii) keeping relevant records and technical documentation.
- Requiring organisations to be transparent with users about the fact that they will be using AI.
- Establishing an EU AI Board to oversee national EU regulators.

Penalties

There are potential fines of up to 6% of global turnover or €30 million for non-compliance.

Current status

Subject to the outcome of final trilogue discussions, the AI Act could enter into force by the end of 2023. Organisations would then approximately two years until it would come into effect.

Regulating the use of Artificial Intelligence

EU Artificial Intelligence Liability Directive ("AI Directive")

The EU has proposed the AI Directive which aims to create a non-contractual liability regime for victims injured by AI-related products. Its purpose is to modernise the current liability regime to incorporate AI harms, reduce uncertainty, and instil confidence in those interacting with emerging AI technologies.

Who will the AI Directive apply to?

It will apply to providers and users of AI systems that are available or operate within the EU.

Key proposals

- Lowering the evidentiary hurdles for victims injured by AI-related products or services and making it easier to establish claims against an AI developer, provider or user.
- Introducing measures to empower courts in EU member states to compel the disclosure of evidence related to AI systems in certain situations.
- Allowing claims to be brought by a subrogated party or a representative, including by class action.

The AI Directive does not currently address situations where an AI system causes damage but there is no obvious defective product or fault by either the provider or user. However, the European Commission intends to assess the need for no-fault strict liability rules five years after the entry into force of the AI Liability Directive.

Current status

The draft text of the AI Directive needs to be considered and adopted by the European Parliament and Council. Once agreed, it will need to be transposed into national law in EU member states within two years.

Regulating the use of Artificial Intelligence

UK AI Strategy & Policy Paper

The Department for Digital, Culture, Media & Sport ("DCMS") has proposed the introduction of a flexible regulatory regime for AI, focussing on cross-sectoral principles applicable to AI as well as the rand of new and accelerated risks that AI creates.

The cross-sectoral principles proposed by the DCMS will expand on the Organisation for Economic Co-operation and Development's Principles on Artificial Intelligence.

Key proposals

- Ensuring that AI is (i) used safely; (ii) technically secure; (iii) functions as designed; and (iv) appropriately transparent and explainable.
- Embedding considerations of fairness into AI.
- Defining legal persons responsible for AI governance.
- Clarifying routes to redress or contestability.
- Creating AI standards and assurance tools to support the overall framework.
- Involving a number of regulators in the DCMS's regime, including the ICO, CMA, MHRA and EHRC.

The overall purpose of the proposals are to help create a "nimble regulatory framework" to help the UK become a hub for AI and innovation more broadly.

Current status

The DCMS is in the process of considering feedback from a public consultation before making a legislative proposal. Initially this will be in the form of a White Paper expected in the first quarter of 2023.

Cyber security

NIS2 Directive ("NIS2")

The NIS2 will expand the scope of the current NIS Directive in response to the increase in cyberattacks and threats. It aims to strengthen security requirements, streamline reporting obligations, tackle supply chain security issues and introduce stricter supervisory and enforcement mechanisms.

Who will the NIS2 apply to?

It will apply to both "essential sectors" such as health, energy, transport, banking and digital infrastructure and "important sectors" such as food production, waste management, manufacturers of medical devices and postal services.

Key provisions

- Places direct obligations on "management bodies" responsible for their organisation's compliance. This could lead to fines and temporary bans from discharging such managerial functions.

- Cyber risk management measures must be implemented such as carrying out due diligence of third-party suppliers and services.

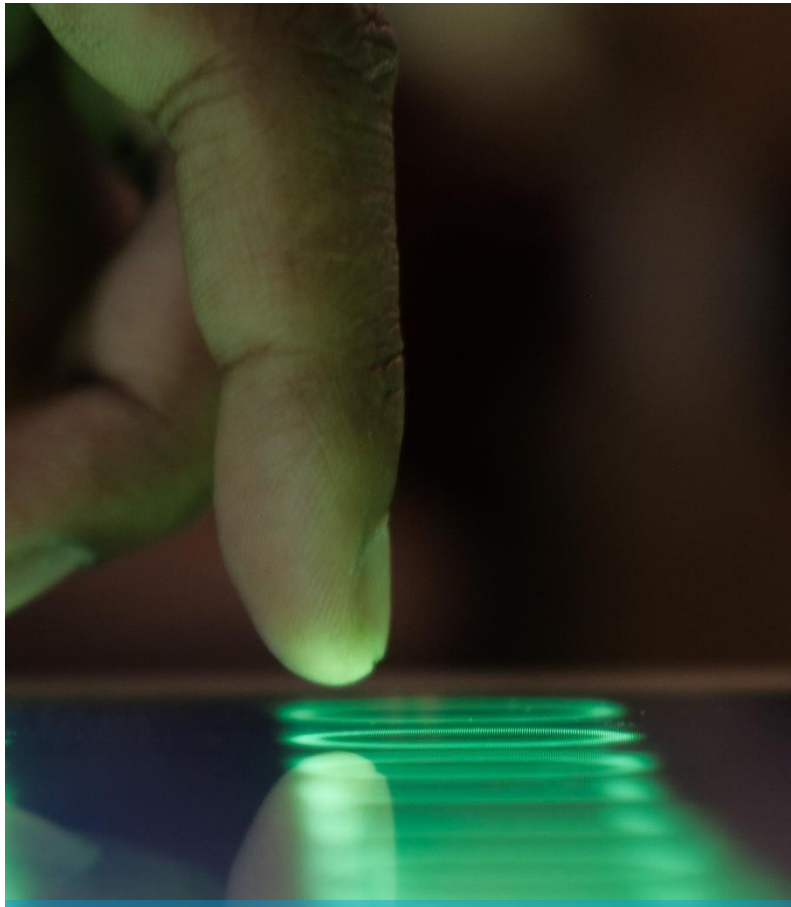
- New reporting requirements require an initial notification within 24 hours of becoming aware of certain incidents/threats, followed by "intermediate" and "final" reporting obligations.

Penalties

Member States will be granted the discretion to set proportionate and dissuasive penalties for breaches, and to issue administrative fines for certain breaches of up to the higher of €10 million or 2% of worldwide turnover.

Current status

The NIS2 came into force on 16 January 2023. EU Member States have until 17 October 2024 to incorporate the NIS2 into national law.



***"With the agreement of NIS2, we modernise rules to secure more critical services for society and economy. This is therefore a major step forward"* - Thierry Breton**

(Commissioner for the Internal Market)

Cyber security

Cyber Resilience Act ("CRA")

The official proposal of the CRA has been published by the European Commission. The focus of the CRA is to provide cybersecurity requirements for "products with digital elements" and strengthen cybersecurity rules to ensure that hardware and software products are more secure.

Who will the CRA apply to?

The CRA will be the first EU-wide legislation of its kind and shall introduce cybersecurity requirements that are mandatory for products with digital elements throughout their lifecycle. It will apply to distributors and importers of digital products.

Key proposals

Under the CRA, manufacturers of in-scope products will be required to meet new reporting obligations and assess cybersecurity risks in relation to all aspects of a product. It will apply to products placed on the EU market, irrespective of where they are manufactured, and products designated as critical will be subject to more onerous obligations.

Penalties

Potential fines of up to €15 million or 2.5% of global annual turnover (whichever is higher) for non-compliance.

Current status

A revised draft of the CRA was published by the Council of the EU on 18 November 2022 and EU Member States were invited to submit written statements on the updated draft. The CRA is not expected to come into force until 2024 or 2025.

"The Cyber Resilience Act is our answer to modern security threats that are now omnipresent through our digital society." **- Margaritis Schinas**

(Vice-President for Promoting our European Way of Life)

Cyber security

UK Proposal for legislation to improve the UK's cyber resilience

As part of the UK government's £2.6 billion National Cyber Strategy, DCMS has proposed updating the Network and Information Systems Regulations ("NIS Regulations") to increase the cybersecurity reporting requirements for essential service providers.

Who will the NIS regulations apply to?

The proposals would expand the scope of the NIS Regulations to additional service providers and would require large companies to report all cyber incidents to the relevant regulators.

Key provisions

- A wider application to the most critical digital service providers in the UK's economy, including providers of managed IT and outsourced services, cloud computing and online search engines.
- New requirements for organisations in scope to improve their cyber incident reporting through sector regulators such as Ofcom or Ofgem and the ICO.
- A new cost recovery system for regulators enforcing the NIS Regulations that is more transparent and takes into account the wider regulatory burdens, company size, and other factors to reduce taxpayer burden.

Penalties

Organisations that fail to put in place effective cyber security measures can be fined as much as £17 million for non-compliance.

Current status

The government announced on 30 November 2022 that it will proceed with its proposals "*as soon as parliamentary time in allows*".

"We are strengthening the UK's cyber laws against digital threats. This will better protect our essential and digital services and the outsourced IT providers which keep them running."
– Julia Lopez

(Minister for Digital, Culture, Media and Sport)

Cyber security

UK Product Security and Telecommunications Infrastructure Act 2022 ("PSTIA")

The PSTIA is set to impose new security-related requirements to protect users and enhance the security of IoT connected products made available in the UK, including both physical shops and online retailers.

Who will the PSTIA apply to?

The PSTIA applies to organisations that make, import or distribute any internet-connectable products to UK consumers (and UK business, in certain circumstances).

Key provisions

Under the PSTIA, manufacturers, importers and distributors have a duty to:

- Comply with security requirements (yet to be defined in subsidiary regulations) and provide a "statement of compliance" with these requirements.
- Investigate and act upon potential compliance failures, and to take appropriate actions (e.g. notifications, discontinuing product availability, and remediation).
- Maintain records of compliance failures and investigations.

Importers and distributors also have duties not to supply products believed to be non-compliant and to take all reasonable steps to prevent the product from being made available to customers in the UK.

Penalties

Fines of up to either £10 million or 4% of qualifying worldwide revenue, whichever is the greater. With potential £20,000 fines per day for failing to remediate when notified.

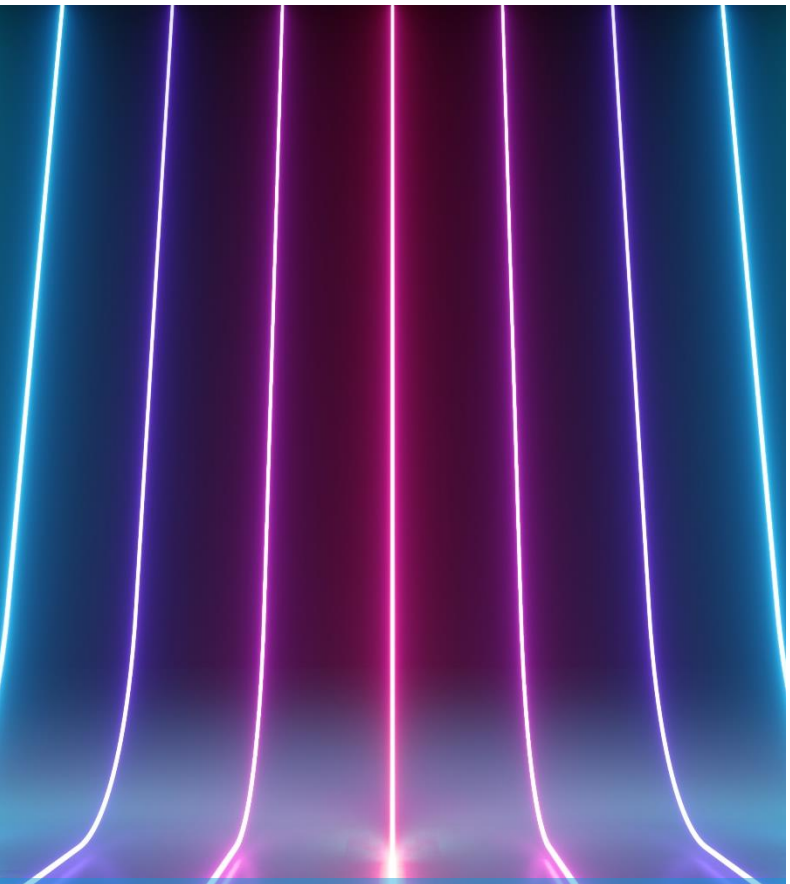
Current status

The PSTIA became law in December 2022 but only a limited number of provisions came into force. The subsidiary regulations are yet be issued, which the government have assured will apply after a minimum 12 months lead-in period.

***"The legislation will also strengthen cyber protection to make sure the UK has the strongest security regime for smart tech in the world."* – Julia Lopez**

(Minister for Digital, Culture, Media and Sport)

Technology & data



‘It is very rare to find an external legal team that not only provides excellent legal advice, but provides excellent practical legal advice. Too often, external firms simply recite the law, and do not apply it to the situation at hand.’

Legal 500 UK, 2023

Our expertise

Our expert team has an extensive track record advising clients on their data, IT and digital transformation projects, across various sectors and industries including retail and leisure, financial services, and luxury goods.

We have significant experience advising on complex IT and digital transformation projects, and on the provision, procurement and deployment of software (including "as a service"), and new disruptive technologies such as AI and machine learning. We cover the whole lifecycle, from advising on IP creation and protection, to structuring sales with end users.

Our data team advises clients in relation to all aspects of data protection and information law, ranging from conducting comprehensive data protection audits and drafting policies and agreements to advising on individual subject access requests and complaints. We advise clients operating at the cutting edge of technology.

‘The ‘incredibly responsive, personable and efficient’ Stephenson Harwood’
Legal 500 2022, Data protection

Key contacts

Simon Bollans
Partner, Technology

T: +44 20 7809 2668
E: simon.bollans@shlegal.com

Katie Hewson
Partner, Data Protection

T: +44 20 7809 2374
E: katie.hewson@shlegal.co

Our wider team in the UK and EU

Boriana Guimberteau
Partner

E: boriana.guimberteau@shlegal.com

Jean-Julien Lemonnier
Partner

E: jj.lemonnier@shlegal.com

Michael Bywell
Partner

E: Michael.Bywell@shlegal.com

Nic McMaster
Associate

E: nic.mcmaster@shlegal.com

Martha Hampton
Associate

E: Martha.Hampton@shlegal.com

Joseph Samuelson
Associate

E: Joseph.Samuelson@shlegal.com