





# Forthcoming legislation: a quick guide

Instrument	What does it do?	When will it apply?¹
 <b>Digital Services Act</b>	<ul style="list-style-type: none"> <li>Regulates online intermediaries with a view to creating a trustworthy online environment.</li> <li>Clarifies and amends current safe harbour rules that shield online hosts from liability for third party illegal content on their services. Amends the current e-commerce Directive.</li> <li>Imposes obligations on all online intermediaries offering services into the EU single market (whether established within or outside the EU). online marketplaces, app stores, online hosts,</li> <li>Enables reporting of illegal content, goods or services on online platforms</li> <li>Imposes due diligence obligations for platforms and stronger obligations for very large platforms and very large online search engines, where the most serious harms occur.</li> <li>Requires non-EU intermediary services providers to have a legal representative in the EU. Legal representatives can be held liable for non-compliance.</li> <li>Enables authorities to protect citizens by supervising platforms and enforcing rules.</li> </ul>	<p>The majority of the provisions will apply 15 months after entry into force (expected imminently) or on 1 January 2024, whichever is the later.</p>
 <b>Digital Markets Act</b>	<ul style="list-style-type: none"> <li>Ensures fair and open digital markets by regulating large online platforms (for example cloud computing services, online social networking services and online search engines) which offer services to the EU market.</li> <li>Prevents large platforms from over-promoting their own products, limiting payment methods to their own mechanisms, re-using personal data collected in the course of providing a particular service for the purposes of another service, imposing unfair conditions on business-users, pre-installing certain software applications, restricting business users of platforms and selling different items as a package.</li> </ul>	<p>March 2023</p>
 <b>AI Act</b>	<ul style="list-style-type: none"> <li>Creates rules that will affect anybody who places AI on the market in the EU (or develops AI for the EU market), uses AI in the EU, or uses the outputs of AI in the EU.</li> <li>Classifies AI systems depending on level of risk associated with planned use.</li> <li>Certain AI uses will be banned outright. Others will have to meet certain standards in order to gain access to the EU market.</li> </ul>	<p>Still under negotiation. Proposal is for it to apply two years after it comes into force.</p>
 <b>AI Liability Directive</b>	<ul style="list-style-type: none"> <li>Complements the AI Act by facilitating fault-based civil liability claims for victims of AI-related damage, enabling them to get compensation.</li> </ul>	<p>The proposal was announced in September 2022 and has yet to be negotiated by the EU institutions. The proposed deadline for implementation by Member States is two years after entry into force.</p>

1. Some EU instruments enter into force at a particular time but do not apply (or in other words have legal effect) until a later time.

Instrument	What does it do?	When will it apply? <sup>1</sup>
<b>Data Governance Act</b> 	<ul style="list-style-type: none"> <li>• Introduces measures to boost the EU data economy and support a single European data space.</li> <li>• Creates a framework to encourage safe and compliant re-use of public sector data that is subject to third party rights, such as IP, trade secrets or rights in personal data (Protected Data). Restricts transfers of non-personal Protected Data to third countries. Transfers may only take place subject to certain requirements such as putting in place model contract clauses.</li> </ul>	September 2023
<b>Data Act</b> 	<ul style="list-style-type: none"> <li>• While the Data Governance Act creates the processes and structures to facilitate data sharing by companies, individuals and the public sector, the Data Act clarifies who can create value from data and under which conditions.</li> <li>• Contains new rules on who can use and access data generated in the EU across all economic sectors.</li> <li>• Ensures fairness in the digital environment, encourages a competitive data market, opens opportunities for data-driven innovation and makes data more accessible for all thereby leading to new, innovative services and more competitive prices for aftermarket services and repairs of connected objects.</li> </ul>	Currently being negotiated by the EU institutions. The proposal is for the Act to apply a year after entry into force.
<b>ePrivacy Regulation</b> 	<ul style="list-style-type: none"> <li>• This instrument was meant to come in at the same time as the GDPR, but has been delayed by a lack of consensus amongst EU legislators.</li> <li>• Repeals and replaces the eprivacy Directive.</li> <li>• Would regulate telecoms operators as well as machine-to-machine and Internet of Things data transmitted via public networks.</li> <li>• May relax rules relating to consent for non-essential cookies and enable reliance on the soft opt-in for direct marketing in a wider range of circumstances.</li> </ul>	Currently in the final stages of being negotiated as between the European Commission, Parliament and Council (known as trilogue). Once adopted it will apply after two years).
<b>Network &amp; Information Security Directive<sup>2</sup></b> 	<ul style="list-style-type: none"> <li>• Repeals and replaces the current NIS directive.</li> <li>• Aimed at providing a high common level of cybersecurity in the EU, following growing threats posed with digitalisation and a surge in cyber-attacks.</li> <li>• Strengthens existing security requirements, addresses the security of supply chains, streamlines reporting obligations, and introduces more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU.</li> <li>• Applies to a wider range of entities than the current NIS Directive including essential entities (for example energy, transport, financial market infrastructures, health, manufacture of pharmaceutical products including vaccines) and important entities (such as postal and courier services, waste management, chemicals).</li> </ul>	Currently being negotiated by the EU institutions. The proposed deadline for implementation by Member States is 18 months after entry into force.
<b>Cyber Resilience Act</b> 	<ul style="list-style-type: none"> <li>• Complements the revised NIS directive.</li> <li>• Guarantees harmonised rules when bringing to market products or software with a digital component.</li> <li>• Provides a framework of cybersecurity requirements governing the planning, design, development and maintenance of such products, with obligations to be met at every stage of the value chain.</li> <li>• Imposes an obligation to provide duty of care for the entire lifecycle of products.</li> </ul>	Recently proposed – needs to be negotiated by the EU institutions. The proposal is that the majority of obligations in the Act will become applicable 24 months after entry into force (reporting obligations on manufacturers, may apply 12 months after entry into force).

2. Similar changes are under consideration in the UK but no legislative proposals have yet been brought forward.

Instrument	What does it do?	When will it apply? <sup>1</sup>
 <p><b>Digital Operational Resilience Act</b></p>	<ul style="list-style-type: none"> <li>• Part of the Digital finance package - a package of measures to further enable and support the potential of digital finance in terms of innovation and competition while mitigating risks.</li> <li>• Puts in place a detailed and comprehensive framework on digital operational resilience for EU financial entities.</li> <li>• Enhances and streamlines the financial entities' conduct of Information and Communication Technologies ("ICT") risk management, establishes a thorough testing of ICT systems, increases supervisors' awareness of cyber risks and ICT-related incidents faced by financial entities.</li> <li>• Introduces powers for financial supervisors to oversee risks stemming from financial entities' dependency on ICT third-party service providers.</li> <li>• Creates a consistent incident reporting mechanism that will help reduce administrative burdens for financial entities, and strengthen supervisory effectiveness.</li> </ul>	<p>Recently proposed – needs to be negotiated by the EU institutions. Current proposal is that it should apply 12 months after entry into force.</p>
 <p><b>Data Protection and Digital Information Bill</b></p>	<ul style="list-style-type: none"> <li>• Amends the UK GDPR in order to update and simplify the UK's data protection framework with a view to reducing burdens on organisations while maintaining high data protection standards.</li> </ul>	<p>The legislation has been introduced in Parliament but there is uncertainty as to whether it will proceed following the change of administration in the UK.</p>
 <p><b>Retained EU Law (Revocation and Reform) Bill</b></p>	<ul style="list-style-type: none"> <li>• Sunsets all of the law saved when the UK left the EU by the end of 2023, unless Ministers specify that particular pieces of legislation should remain on the statute book (the UK GDPR and the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR") fall within the scope of the sunset provisions).</li> <li>• Changes how any law kept on the statute book is interpreted (including the UK's data protection frameworks).</li> <li>• Gives Ministers wide-ranging powers to restate, replace or revoke this body of law. Replacement legislation for the UK GDPR and PECR could be made using these powers.</li> </ul>	<p>Likely by summer 2023, although the Bill is likely to be controversial and may not survive in its current form.</p>
 <p><b>Online Safety Bill</b></p>	<ul style="list-style-type: none"> <li>• Establishes a new regulatory regime to address illegal and harmful content online, with the aim of preventing harm to individuals in the United Kingdom.</li> <li>• Imposes duties of care in relation to illegal content and content that is harmful to children on providers of internet services which allow users to upload and share user-generated content ("user-to-user services") and on providers of search engines which enable users to search multiple websites and databases ("search services").</li> <li>• Imposes duties on such providers in relation to the protection of users' rights to freedom of expression and privacy.</li> <li>• Confers powers on the Office of Communications (Ofcom) to oversee and enforce the new regulatory regime (including dedicated powers in relation to terrorism content and child sexual exploitation and abuse (CSEA) content), and requires Ofcom to prepare codes of practice to assist providers in complying with their duties of care.</li> </ul>	<p>Currently going through UK Parliament although progress has stalled in light of change of administration. Expected to proceed (subject to potential changes).</p>