Regulatory Landscape - Cross-Cutting

This section lists out the regulations and directives that apply to all financial services institutions, including obligations related to data protection, environmental, social and governance (ESG), operational resilience and other corporate governance related matters.

Title	Key dates	Key Information
Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR)	Publication date: May 4, 2016 Effective date: May 24, 2016 Application date: May 28, 2015	This regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. In particular, the regulation applies to the processing of personal data wholly or partially by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. The regulation provides requirements on: • Principles relating to the processing of data. • The lawfulness of processing. • Conditions for consent, including conditions for a child's consent. • The rights of the data subject. • Information and access to personal data. • Controllers and processors. The regulation repeals Directive 95/46/EC.
Directive 2022/2464 (Corporate Sustainability Reporting Directive – CSRD)	Publication date: December 16, 2022 Effective date: January 5, 2023 Member state transposition deadline: July 6, 2024 Application date:	This directive establishes updated rules concerning corporate sustainability reporting. In doing so, it lays down uniform requirements for large companies and listed small and medium-sized enterprises (SMEs) to disclose information on the environmental, social and governance (ESG) risks they face, as well as how their activities impact people and the environment. The directive introduces several new provisions and requirements, including: • European Sustainability Reporting Standards (ESRS). Mandates that in-scope companies report sustainability information in accordance with detailed, standardised European frameworks. • Double materiality. Requires companies to report on both how sustainability issues affect their business development and performance (financial

	January 1, 2024	materiality) and how their business activities impact people and the environment (impact materiality). • Expanded scope. Broadens the reporting mandate beyond the previous Non-Financial Reporting Directive (NFRD) to cover all large EU companies, all companies listed on EU-regulated markets (excluding micro-enterprises), and certain non-EU companies generating significant net turnover in the EU. • Mandatory assurance. Introduces a requirement for an independent third-party audit (assurance) of the reported sustainability information to ensure accuracy and reliability. • Digital tagging. Requires companies to prepare their management report in a specific digital format and digitally tag their sustainability disclosures to make them machine-readable. The directive also amends several legislations: • Directive 2013/34/EU. • Directive 2004/109/EC. • Directive 2006/43/EC. • Regulation (EU) No. 537/2014.
Regulation (EU) 2022/2554 (Digital Operational Resilience Act – DORA)	Publication date: December 27, 2022 Effective date: January 16, 2023 Application date: January 17, 2025	This regulation establishes a uniform framework for the digital operational resilience of the financial sector. In doing so, it lays down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities (such as banks, insurance companies and investment firms) to ensure they can withstand, respond to, and recover from all types of information and communication technology (ICT) disruptions and cyber threats. The regulation provides for the following requirements: • ICT risk management. This includes establishing sound internal governance and control frameworks, identifying critical dependencies and maintaining resilient, up-to-date ICT systems. • ICT-related incident management, classification and reporting. This includes establishing processes to monitor, log, classify and promptly report major ICT-related incidents to the relevant competent authorities. • Digital operational resilience testing. This involves periodically testing ICT tools and systems for vulnerabilities, including conducting advanced threat-led penetration testing (TLPT) based on an entity's size and risk profile. • ICT third-party risk management. This introduces strict rules for monitoring

		risks stemming from outsourced ICT services and establishes a pan-European oversight framework for critical ICT third-party service providers (CTPPs), such as cloud service providers. • Information sharing. This allows financial entities to voluntarily establish secure arrangements to exchange cyber threat information and intelligence amongst themselves to enhance collective resilience. The regulation also amends several pieces of legislation: • Regulation (EC) No. 1060/2009. • Regulation (EU) No. 648/2012. • Regulation (EU) No. 600/2014. • Regulation (EU) No. 909/2014. • Regulation (EU) 2016/1011.
Directive (EU) 2022/2556	Publication date: December 27, 2022 Effective date: January 16, 2023 Member state transposition deadline: January 17, 2025 Application date: January 17, 2025	This directive accompanies Regulation (EU) 2022/2554 (Digital Operational Resilience Act – DORA). It establishes a consistent legal framework by amending several existing EU financial services directives to align them with the new uniform requirements for digital operational resilience. In doing so, it ensures that information and communication technology (ICT) risks are explicitly and uniformly addressed across the varying regulatory frameworks governing the financial sector. The directive amends several legislations: • Directive 2009/65/EC. • Directive 2009/138/EC. • Directive 2011/61/EU. • Directive 2013/36/EU. • Directive 2014/59/EU. • Directive 2014/65/EU. • Directive (EU) 2015/2366. • Directive (EU) 2016/2341.
Regulation 2024/3005 (Environmental, Social and Governance (ESG) Ratings Activity – ESGRA)	Publication date: December 12, 2024 Effective date: January 2, 2025 Application date:	This regulation establishes a mandatory framework for the transparency and integrity of environmental, social and governance (ESG) rating activities. In doing so, it lays down uniform rules for providers of ESG ratings operating in the EU to strengthen the reliability, comparability and independence of ESG ratings, while preventing potential conflicts of interest and mitigating greenwashing risks within the sustainable finance ecosystem.

	July 2, 2026	The regulation provides for the following requirements: • Authorisation and supervision. This requires ESG rating providers established in the EU to be authorised and supervised by the European Securities and Markets Authority (ESMA) and establishes strict recognition and endorsement regimes for third-country providers. • Transparency and methodology disclosures. This mandates providers to publish detailed, standardised information on their websites regarding the specific methodologies, models, data sources and key assumptions used to generate their ESG ratings. • Separation of business and activities. This introduces strict governance requirements to prevent conflicts of interest, generally prohibiting ESG rating providers from simultaneously engaging in certain other activities such as consulting, issuing credit ratings, auditing, or banking. • Fact-checking mechanism. This grants rated entities or issuers the opportunity to verify the specific datasets used by the provider and highlight any factual errors prior to the initial issuance of the rating, acting purely as a data-verification tool without allowing the entity to influence the rating's methodology or outcome. The regulation also amends: • Regulation (EU) 2019/2088. • Regulation (EU) 2023/2859.
Directive 2002/87/EC (Financial Conglomerates Directive – FCD)	Publication date: February 11, 2003 Effective date: February 11, 2003 Member state transposition deadline: August 10, 2004 Application date: August 10, 2004	This directive establishes a framework for the supplementary supervision of credit institutions, insurance undertakings and investment firms that are part of a financial conglomerate. In doing so, it addresses loopholes in sectoral financial legislation by ensuring that large financial groups with significant cross-sectoral activities are subject to group-wide prudential oversight. The directive provides for the following requirements: • Establishes specific quantitative thresholds and criteria to identify which financial groups qualify as conglomerates and must be subject to supplementary supervision. • Requires conglomerates to maintain adequate capital at the group level to prevent "double gearing" (the multiple use of the same capital to cover different risks across various entities within the group) and to avoid the inappropriate intra-group creation of own funds.

		• Mandates the monitoring, reporting and supervision of significant risk concentrations and intra-group transactions to mitigate the risk of financial contagion spreading from one entity to another. • Requires the implementation of sound corporate governance, robust risk management processes and adequate internal control mechanisms at the level of the financial conglomerate. • Mandates the appointment of a single designated supervisory authority (the "coordinator") to oversee and coordinate the group's supplementary supervision, facilitating structured cooperation and information sharing among all relevant national competent authorities. The directive also amends several pieces of legislation: • Directive 73/239/EEC. • Directive 79/267/EEC. • Directive 92/49/EEC. • Directive 92/96/EEC. • Directive 93/6/EEC. • Directive 93/22/EEC.
Regulation (EU) 2019/2088 (Sustainable Finance Disclosure Regulation – SFDR)	Publication date: December 9, 2019 Effective date: December 29, 2019 Application date: March 10, 2021	This regulation lays down harmonised rules for financial market participants and financial advisers on transparency with regard to the integration of sustainability risks and the consideration of adverse sustainability impacts in their processes, as well as the provision of sustainability-related information with respect to financial products. The regulation provides for the following requirements: • Integration of sustainability risks. This requires entities to publish written policies on their websites detailing how they integrate sustainability risks into their investment decision-making processes or investment advice. • Principal adverse impacts (PAI). This mandates the disclosure of how entities consider the principal adverse impacts of their investment decisions on broader sustainability factors (such as environmental, social and employee matters, respect for human rights, and anti-corruption) at both the entity and individual financial product levels. • Product classification and specific disclosures. This introduces a categorisation system for financial products, requiring tailored pre-contractual, website, and periodic reporting disclosures based on their level of sustainability ambition. • Remuneration policies. This requires entities to include information in their remuneration policies on how those policies are consistent with the

		integration of sustainability risks, and to publish that transparency on their websites.
Regulation (EU) No. 1093/2010 (European Banking Authority Regulation – EBAR)	Publication date: December 15, 2010 Effective date: December 16, 2010 Application date: January 1, 2011	This regulation establishes the European Supervisory Authority (European Banking Authority), commonly known as the EBA. In doing so, it creates a decentralised EU agency tasked with ensuring effective and consistent prudential regulation and supervision across the European banking sector. The regulation forms a core part of the European System of Financial Supervision (ESFS). This regulation amends Decision No. 716/2009/EC. It also repeals Commission Decision 2009/78/EC.
Directive 2004/25/EC (Takeover Directive – TD)	Publication date: April 30, 2004 Effective date: May 20, 2004 Member state transposition deadline: May 20, 2006 Application date: May 20, 2006	This directive establishes a framework for takeover bids involving the securities of companies governed by the laws of member states, where all or some of those securities are admitted to trading on a regulated market within the EU. It lays down minimum guidelines to protect the interests of minority shareholders, employees, and other stakeholders when corporate control changes hands, ensuring that takeovers are conducted in a transparent, orderly, and fair manner across the single market.
Regulation (EU) 2023/2859 (European Single Access Point (ESAP) Regulation – ESAPR)	Publication date: December 20, 2023 Effective date: January 9, 2024 Application date: Phased application starting from July 10, 2026 (with the platform mandated to go live by July 10,	This regulation establishes the European Single Access Point (ESAP), a flagship initiative of the EU's Capital Markets Union Action Plan. In doing so, it lays down rules for creating a centralised digital platform that provides free, user-friendly, and electronic access to public financial, non-financial, and sustainability-related information about EU companies and investment products. The overall aim is to boost the visibility of EU businesses (including SMEs) to domestic and international investors, facilitating better decision-making and cross-border investments.

	2027)	
Directive (EU) 2022/2555 (Network and Information Security Directive II – NIS II) Vixio – Mapping EU Legislation: Directive (EU) 2022/2555 (FS Only)	Publication date: December 27, 2022 Effective date: January 16, 2023 Member state transposition deadline: October 17, 2024 Application date: October 18, 2024	This directive establishes a comprehensive framework to achieve a high common level of cybersecurity across the European Union. In doing so, it significantly expands the scope of the original NIS Directive to cover medium and large entities operating in a wider range of critical sectors (such as energy, transport, banking, healthcare, digital infrastructure and public administration). The directive provides for the following requirements: • Categorises in-scope organisations into "essential" and "important" entities based on their sector and criticality, subjecting them to different supervisory regimes and penalty structures. • Mandates entities to implement robust technical, operational and organisational measures. This includes risk analysis, incident handling, supply chain security, business continuity, encryption and basic cyber hygiene practices. • Introduces strict, multi-stage notification requirements for significant cyber incidents. Entities must submit an early warning to their national authority within 24 hours of becoming aware of the incident, followed by an incident update within 72 hours, and a comprehensive final report within one month. The directive amends the following legislation: • Regulation (EU) No. 910/2014. • Directive (EU) 2018/1972. This directive repeals the following: • Directive (EU) 2016/1148.
Regulation (EU) 2024/1689 (Artificial Intelligence Act – AIA)	Publication date: July 12, 2024 Effective date: August 1, 2024 Application date: Phased application starting from February 2, 2025.	This regulation establishes a comprehensive, harmonised legal framework for the development, placing on the market, putting into service and use of artificial intelligence (AI) systems within the Union. In doing so, it takes a risk-based approach to ensure that AI systems are safe, transparent and respect fundamental rights, democracy and the rule of law, while simultaneously promoting innovation and investment in trustworthy AI across the single market. The regulation also amends several pieces of legislation: • Regulation (EC) No. 300/2008. • Regulation (EU) No. 167/2013.

	Full application from August 2, 2026.	• Regulation (EU) No. 168/2013. • Regulation (EU) 2018/858. • Regulation (EU) 2018/1139. • Regulation (EU) 2019/2144. • Directive 2014/90/EU. • Directive (EU) 2016/797. • Directive (EU) 2020/1828.
Directive (EU) 2019/882 (European Accessibility Act – EAA)	Publication date: June 7, 2019 Effective date: June 27, 2019 Member state transposition deadline: June 28, 2022 Application date: June 28, 2025	This directive establishes a harmonised legal framework to improve the accessibility of certain everyday products and services across the European Union. The directive provides for the following requirements: • Mandates strict accessibility requirements for specific hardware placed on the market, including computers and operating systems, smartphones, payment terminals, ATMs, ticketing and check-in machines, e-readers and interactive television equipment. • Mandates accessibility requirements for essential digital and consumer services. • Requires products to be designed and produced to maximise their use by people with disabilities, with detailed rules covering user interfaces, functionality and accessible packaging. Services must provide accessible information, navigable websites and compatible mobile applications.
Directive 2014/95/EU (Non-Financial Reporting Directive – NFRD)	Publication date: November 15, 2014 Effective date: December 5, 2014 Member state transposition deadline: December 6, 2016 Application date: Financial years starting on or after January 1, 2017	This directive establishes rules regarding the disclosure of non-financial and diversity information by certain large undertakings and groups. In doing so, it lays down minimum requirements for large public-interest entities (such as listed companies, banks and insurance companies) to disclose information on the way they operate and manage social and environmental challenges. The overall aim is to improve corporate transparency, relevance, consistency and comparability of non-financial information across the EU, encouraging companies to develop a responsible approach to business. The directive amends Directive 2013/34/EU.

Regulation (EU) 2024/2847 (Cyber Resilience Act – CRA)	Publication date: November 20, 2024 Effective date: December 10, 2024 Application date: December 11, 2027	This regulation establishes horizontal cybersecurity requirements for products with digital elements (both hardware and software) placed on the EU market. In doing so, it lays down uniform rules to ensure that manufacturers design, develop and produce secure digital products, and that they maintain this security throughout the product's entire lifecycle. The regulation provides for the following requirements: • Mandates that products are designed and developed to protect against unauthorised access, safeguard the confidentiality, integrity and availability of data, and minimise the impact of potential cyber incidents right out of the box. • Requires manufacturers to actively manage vulnerabilities throughout the product's support period. This includes deploying automatic security updates (where feasible and separate from feature updates) and proactively informing users about available remedies. • Introduces strict, rapid reporting obligations, requiring manufacturers to notify relevant national authorities and the European Union Agency for Cybersecurity (ENISA) of actively exploited vulnerabilities or severe security incidents within 24 hours of becoming aware of them. The regulation amends the following legislation: • Regulation (EU) No. 168/2013. • Regulation (EU) 2019/1020. • Directive (EU) 2020/1828.
Regulation (EU) 2023/2854 (Data Act – DA)	Publication date: December 22, 2023 Effective date: January 11, 2024 Application date: September 12, 2025	This regulation establishes harmonised rules on fair access to and use of data across all economic sectors. In doing so, it clarifies who can create value from data generated by connected products (the Internet of Things) and related services. The regulation amends the following legislation: • Regulation (EU) 2017/2394. • Directive (EU) 2020/1828.