THE REVIEW OF
BANKING & FINANCIAL SERVICES
A PERIODIC REVIEW OF SPECIAL LEGAL DEVELOPMENTS AFFECTING LENDING AND OTHER FINANCIAL INSTITUTIONS

Vol. 41 No. 3 March 2025

AI AND TECH REGULATION FOR THE FINANCIAL SECTOR

Financial institutions are typically familiar with compliance requirements because they have been heavily regulated in most places. In addition to sector-specific regulations, financial services businesses increasingly must also address technology regulations. This article explains the approaches to technology and AI regulation in the European Union and in the United States, provides examples of technology regulation in the European Union, and concludes with practical recommendations.

By Lothar Determann and Michaela Nebel *

Businesses must think globally but comply locally.[1] On the one hand, they must consider opportunities, risks, and trends around the world, including with respect to new technologies. At the same time, they need to comply with laws and regulations that countries, states, counties, and cities prescribe and enforce locally. Financial institutions face distinct challenges with respect to information technology regulations compared to finance-specific regulation, given their different subject matter, mechanisms, and territorial scope, highlighted in Part I. Lawmakers in Europe, in the US, and elsewhere have traditionally taken different approaches with respect to AI and other information technology regulations, examined in Part II and III respectively. Examples of new technology regulations that businesses in the financial sector have to grapple with are introduced in Part IV, as a basis for recommended approaches for financial sector businesses to comply with AI and information technology regulations in Part V.

I. FINANCIAL INSTITUTIONS, TECHNOLOGY, COMPANIES,FINTECHS, AND REGULATIONS

Banks and other traditional financial institutions tend to be well adapted to complying with local laws, because they have long been heavily regulated in most places. To engage in most banking and many finance activities, businesses require licenses from specialized financial regulators that watch over particular territories. Financial institutions traditionally incorporate entities with physical offices and employees where they operate.Global financial groups that act in multiple jurisdictions often set up separate subsidiary companies

[1] On the origins of the motto "think globally, act locally", *see* Daniel Tarantola, *Thinking Locally, Acting Globally?*, 103 American Journal of Public Health 11, Nov. 2013, at 1926, https://doi.org/10.2105/AJPH.2013.301636.

* *PROF. DR. LOTHAR DETERMANN is a partner in Baker McKenzie's Palo Alto office where he practices technology law and teaches data privacy, computer, and AI law at the Free University Berlin and Berkeley School of Law. DR. MICHAELA NEBEL is a partner in Baker & McKenzie's Frankfurt office where she advises companies on data, cybersecurity, and AI law, with a strong focus on data protection law and data dispute matters. Their e-mail addresses are michaela.nebel@bakermckenzie.com and lothar.determann@bakermckenzie.com.*

FORTHCOMING

- ***WHAT TO EXPECT IN BANK REGULATION IN 2025***

RSCR Publications LLC Published 12 times a year by RSCR Publications LLC. Executive and Editorial Offices, 2628 Broadway, Suite 29A, New York, NY 10025-5055. Subscription rates: $650 per year in U.S., Canada, and Mexico; $695 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and full-time teachers. For subscription information and customer service call (866) 425-1171 or visit our Web site at www.rscrpubs.com. General Editor: Michael O. Finkelstein; tel. 212-876-1715; e-mail mofinkelstein@gmail.com. Associate Editor: Sarah Strauss Himmelfarb; tel. 301-294-6233; e-mail shimmelfarb@comcast.net. To submit a manuscript for publication contact Ms. Himmelfarb. ISSN: 1051-1741.

that focus their business on territories where they obtain licenses from local regulators.

Technology companies, by contrast, can access world markets remotely, without local presences, and in many places without a need to obtain local licenses. OpenAI was a small start-up company with a few hundred employees in San Francisco when it launched ChatGPT 3.5 in November 2022, which attracted a million users worldwide within five days (and one hundred million users within two months).[2] Information technology businesses have traditionally faced relatively few sectoral regulations. Legislatures tweaked copyright and patent laws to protect intellectual property in computers and software,[3] but hardly regulated information technologies. When the Internet arrived in the 1990s, most democratic countries agreed to let the World Wide Web develop relatively free from regulations to support globalization, free sharing of ideas, worldwide communications, trade, and peace.[4] Not only did they not regulate the Internet initially, but they enacted specific safe harbors from liability and taxation.[5]

More recently, however, lawmakers around the world have unleashed a tsunami of laws and regulations to counter perceived risks of social media, artificial intelligence, and other information technologies.[6] And in Europe and the United States, legislatures and regulators have crafted technology regulations that apply to companies both within and outside their jurisdictions in order to protect local residents. Additionally, the European Union now requires foreign companies to designate local representatives to simplify the enforcement of local laws,[7] a practice that Russia, Turkey, and other countries quickly followed.[8] Additionally, Russia, Kazakhstan, the People's Republic of China, and Indonesia enacted data residency laws,

[2] https://explodingtopics.com/blog/chatgpt-users; https://x.com/gdb/status/1599683104142430208; Kevin Roose, *The Brilliance and Weirdness of ChatGPT*, The New York Times, December 5, 2022, https://www.nytimes.com/2022/12/05/technology/chatgpt-ai-twitter.html.

[3] *See*, for example, Mark A. Lemley, *Convergence in the Law of Software Copyright?*, 10 High Technology L.J. 12 (1995); Mark A. Lemley & Julie E. Cohen, *Patent Scope and Innovation in the Software Industry*, 89 California Law Review 1 (2001); Lothar Determann and David Nimmer, *Software Copyright's Oracle from the Cloud, Software Copyright's Oracle from the Cloud*, 30 Berkeley Tech L. J. 161 (2015).

[4] Lothar Determann, Komnunikationsfreiheit im Internet [Freedom of Communications on the Internet] (1999).

[5] *See*, for example, the Internet Tax Freedom Act, www.congress.gov/108/plaws/publ435/PLAW-108publ435.htm; Section 512 of the U.S. Copyright Act, and Section 230 of the Communications Decency Act; in Europe, the E-commerce Directive [Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')].

[6] Eric Goldman, *Generative AI is Doomed*, http://dx.doi.org/10.2139/ssrn.4802313.

[7] Art. 27 GDPR; Lothar Determann, *Representatives under Art. 27 of the GDPR*, IAPP Advisor (June 12, 2018), https://iapp.org/news/a/representatives-under-art-27-of-the-gdpr-all-your-questions-answered; Art. 13 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC ("Digital Services Act"); Art. 26 (3) seqq. Directive (EU) 2022/2555 of the European Parliament and the Council of 14 December 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 Directive (EU) 2016/1148 ("NIS 2 Directive"); Art. 17 Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online; Art. 22 and Art. 54 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized 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 ("Artificial Intelligence Act").

[8] Additional Article 4 Turkish Federal Law No. 5151: "The Law on Regulation of Broadcasts via Internet and Combating Crimes Committed by the Means of Such Publications" (May 4, 2007), www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf (in Turkish); Russian Federal Law No. 236-FZ: "On the Activities of Persons in the Internet Information and Telecommunications Network on the Territory of the Russian Federation" (July 1, 2021).

requiring that personal data of their citizens be stored locally in their territory to secure government access to such data and favor local information technology businesses.[9]

When financial institutions face compliance requirements under foreign technology laws to designate local representatives or store data locally, they need to tread carefully, because they may subject themselves to license requirements under financial regulations if they set up local presences. Also, they may find the scope, objectives, and mechanisms of technology regulations unfamiliar or even incompatible with other regulatory requirements, given that technology lawmakers often do not consider the special circumstances of financial institutions. For example, obligations under data privacy laws are often at odds with financial sector risk-management requirements and measures against fraud, money laundering, and tax evasion. In fact, financial institutions find themselves frequently in the crosshairs of different laws and regulators, demanding that they protect individual privacy and financial data (under data protection and privacy laws),[10] make financial data more accessible (under competition laws and open banking regulations),[11] profile clients and report tax cheats and criminals to law enforcement authorities (under risk management and anti-money laundering laws),[12] and refrain from profiling clients, except with voluntary consent or other lawful bases (under data protection laws).[13]

Start-up companies entering financial technology (or "fintech") markets to complement or compete with offerings from traditional institutions often try to stay outside the realm of financial regulations. Many fintech companies follow the motto "more tech than fin" and partner with financial institutions that bring licenses and core financial compliance expertise to the table.[14] Yet, the financial institutions in such partnerships must tackle not only compliance with traditional banking regulations, but also mind technology regulations, given that they tend to have deeper pockets and more exposure to regulatory enforcement and private litigation than their fintech partners. In the realm of cryptocurrencies and other blockchain applications, financial institutions face serious challenges to their business models, as well as complex regulatory scenarios.[15]

II. APPROACH TO TECHNOLOGY AND AI REGULATION IN THE EU

European governments follow traditionally a precautionary principle whereby they regulate businesses concerning new technologies early and comprehensively to prevent potential risks of harm.[16] When the German police started using computers to profile residents to identify potential terrorists in the late 1960s, the state of Hessen enacted the first data protection law worldwide to broadly prohibit the

[9] Lothar Determann, *Data Residency Rules Cutting Into Clouds: Impact and Options for Global Businesses and IT Architectures*, Bloomberg BNA Data Privacy & Security Law Report, 16 PVLR 496 (April 3, 2017); Lothar Determann, *How data residency laws can harm privacy, commerce and innovation - and do little for national security*, World Economic Forum (Jun. 9, 2020), www.weforum.org/agenda/2020/06/where-data-is-stored-could-impact-privacy-commerce-and-even-national-security-here-s-why/; Lothar Determann & Michaela Nebel (née Weigl), *Data Residency Requirements Creeping into German Law*, Bloomberg BNA Privacy & Security Law Report, 15 PVLR 529 (Mar. 3, 2016).

[10] *See*, for example, Art. 5 (1) GDPR and Cal. Civ. Code §1798.100(c) contains data minimization and purpose limitation requirements.

[11] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market and Evan Weinberger, CFPB's Open Banking Data Access Controls Fall Short, Banks Say, Bloomberg Data Privacy & Security News, Oct. 31, 2024; *see* Sue McLean, Michaela Nebel, Ben Slinn and Richard Powell, How does PSD2 interplay with the GDPR, September 2020, https://financialinstitutions.bakermckenzie.com/2020/09/24/european-union-how-does-psd2-interplay-with-the-gdpr/.

[12] Elizabeth McCaul, Anti-money laundering and banking supervision, www.bankingsupervision.europa.eu/press/speeches/date/2023/html/ssm.sp230629_1~5a3879b449.en.html.

[13] Art. 6 GDPR.

[14] Lothar Determann & Manuel Lorenz, *Fintechs im Dschungel der Regulierungen* [*Fintechs in the Djungle of Regulation*], Börsenzeitung, April 1, 2017, at 13.

[15] Matthias Arzt and Thomas Richter, International Handbook of Blockchain Law (2nd Ed. 2024); Vincent Pitaro, Navigating the Intersection of Blockchain and Data Privacy Laws, Hedge Fund Law Report 2022, https://www.hflawreport.com/19213926/navigating-the-intersection-of-blockchain-and-data-privacy-laws.thtml.

[16] Lothar Determann, Neue, gefahrverdächtige Technologien als Rechtsproblem [New, potentially dangerous technologies as a legal problem] (1996).

processing of personal data except with lawful bases.[17] Other governments in Europe followed and enacted data protection laws that were harmonized in 1995 in a European Community Data Protection Directive and replaced by a General Data Protection Regulation ("GDPR") in 2016. Financial institutions have always been required to comply with private sector data protection laws. Yet, they were usually not specifically addressed as financial institutions in the generally applicable and broadly worded laws. It took until December 2023 for the Court of Justice of the European Union ("CJEU") to rule, in a case aptly naming the state of Hessen as defendant, that credit agencies engage in automated decision-making when they issue credit scores, because "the probability value established by a credit information agency and communicated to a bank . . . must be qualified in itself as a decision producing vis-à-vis a data subject 'legal effects concerning him or her or similarly significantly [affecting] him or her' within the meaning of Article 22(1) of the GDPR,"[18] thus triggering transparency rights and potentially explicit consent requirements that would seem to have arisen also under predecessor laws for decades.[19]

Financial institutions and other businesses are still barely catching up with the long list of requirements in the GDPR, which was perceived as excessively burdensome, complex, and wordy when it became applicable in 2018 with 88 pages in the Official Journal of the European Union (whereas the predecessor Data Protection Directive filled only 19 pages). Yet, only a few years later, EU lawmakers unleashed a digital strategy with an onslaught of additional data-related regulations on companies: in 2022 a Data Governance Act ("DGA" – 44 pages, effective since 2023), a Digital Markets Act ("DMA" – 66 pages, effective since 2023), a Digital Services Act ("DSA" – 102 pages, generally effective since February 2024), in 2023 a Data Act ("DA" – 71 pages, taking effect in September 2025), and, on August 1, 2024, the Artificial Intelligence Act ("AI Act"– with 144 pages, generally applicable August 2026).[20] Also, cybersecurity legislation was passed, noteworthy in this regard are in particular the NIS 2 Directive (NIS 2 – 73 pages, to be transposed into national law by October 17, 2024)[21] and the Cyber Resilience Act (81 pages, published in the Official Journal of the EU on November 20, 2024). Financial institutions are not the primary addressees of these massive new regulations, but they are called out specifically in some of the new rules.[22] All financial sector businesses should analyze the new rules to identify compliance requirements on their own businesses and also as relevant to their clients, which requires significant efforts given the sheer volume and complexity. On top, the Digital Operational Resilience Act ("DORA" - 79 pages, applicable from January 17, 2025) is a particular piece of legislation for the financial sector.[23]

III. APPROACH TO TECHNOLOGY AND AI LEGISLATION IN THE UNITED STATES

U.S. legislatures have traditionally focused on specific harms, sectors, and situations.[24] In 1970, around the time when the German state of Hessen enacted the world's first broad data protection law, U.S. Congress enacted the Federal Credit Reporting Act ("FCRA") to regulate consumer reports and credit scoring specifically.[25] Congress explicitly decided against enacting broad data protection laws, to avoid stifling

[17] Lothar Determann, *Data Privacy and Data Security Legislation: Policy focus on data processing regulation v. specific individual harms*, in David A. Marcello (ed.), International Legislative Drafting Guidebook: 25th Anniversary Celebration at 189 (Carolina Academic Press: Durham, NC, 2020).

[18] CJEU Case C/2024/913, *Hessen v. SCHUFA Holding AG*, ECLI:EU:C:2023:957 (Jan. 29, 2024), https://curia.europa.eu/juris/documents.jsf?num=C-634/21, at par. 50.

[19] Art. 15 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046, which was based on the French data protection law from 1978, *see* https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf, page 6.

[20] Lothar Determann and Michaela Nebel, *GDPR v. AI Act & Other EU Data Regulation*, Bloomberg Law (April 23, 2024).

[21] Part IV of this Article for more detail.

[22] *See*, for example, recital 158, Art. 17 – 19 of the AI Act; Recitals 17 and 99 of the EU Data Act.

[23] Part IV of this Article for more detail.

[24] Lothar Determann, *Adequacy of data protection in the USA: myths and facts*, 6 International Data Privacy Law, 244 (2016); https://doi.org/10.1093/idpl/ipw011; California Privacy Law – Practical Guide and Commentary, U.S. and State Privacy Law, 5th Ed. (2023), Ch. 1.

[25] Lothar Determann, California Privacy Law – Practical Guide and Commentary, U.S. and State Privacy Law, 5th Ed. (2023), Ch. 2 F.

innovation and economic development,[26] but addressed specific risks resulting from credit scoring much more effectively with a specific law that financial institutions understood well to apply to them.[27]

Over the years since then, however, federal and state legislatures kept piling on specific data privacy laws. After its 2018 enactment and a 2020 ballot initiative in California, businesses are now subject to the California Consumer Privacy Act ("CCPA") that also applies in B2B and employment contexts despite its name, and similarly broad consumer privacy laws in 19 other U.S. states.[28] Banks can rely on some exemptions in state laws with respect to consumer data covered by the Gramm-Leach-Bliley Act ("GLBA"), but need to comply with general privacy laws in commercial lending, digital marketing, and human resource management.[29] U.S. lawmakers created a sprawling thicket of privacy laws that few businesses can comprehend, leave alone comply with, and calls for federal privacy legislation with strong state law preemption have become louder.[30]

Concerning data security, U.S. legislatures and regulators have enacted multiple laws, regulations, and rules prescribing security measures and incident reporting obligations. In 2002, California was the first jurisdiction in the world to pass a law requiring businesses to notify data subjects of data security breaches.[31] Since then, all U.S. states and many other countries have enacted legislation requiring both private and government entities to notify individuals of security breaches involving personally identifiable information. Under the aforementioned GLBA's Safeguards Rule, financial institutions must develop and implement a comprehensive "information security program," develop incident response plans, and notify customers of data security breaches.[32] Moreover, many companies in the financial sector are regulated as "critical infrastructure" and, as such, subject to a multitude of U.S. state and federal cybersecurity laws. In 2022, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA")[33] into law, under which "covered entities" will be required to report cybersecurity incidents and ransom payments within 72 hours to the Cybersecurity and Infrastructure Agency ("CISA").[34] Under the Federal Trade Commission ("FTC") Safeguards Rule,[35] financial institutions must develop, implement, and maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.[36] In November 2023, the New York Department of Financial Services ("NYDFS") amended cybersecurity regulation 23 NYCRR Part 500, which requires New York insurance companies, banks, and other regulated financial services institutions to maintain a cybersecurity program that meets several criteria, and is overseen by senior management.[37] The new amendment not only establishes new reporting obligations, but also requires the establishment of a comprehensive governance system, as well as stricter

[26] Paul Schwartz, *Privacy and Preemption*, Yale L.J., 902 (2009).

[27] Besides the Fair Credit Reporting Act ("FCRA") of 1970, Congress passed other federal financial privacy laws, including within the Gramm-Leach-Bliley Act ("GLBA"), the Fair Debt Collection Practices Act ("FDCPA") and the Right to Financial Privacy Act ("RFPA"); California has enacted analogues to each of these four federal laws, some before and some after Congress acted, plus other California financial privacy laws that do not have a federal equivalent, including the Song-Beverly Credit Card Act and the California Insurance Information and Privacy Protection Act; for more detail, *see* Lothar Determann, California Privacy Law, Ch. 2 (F) (5th Ed. 2023).

[28] Overview from the International Association of Privacy Professionals *at* https://iapp.org/media/pdf/resource_center/us_state_privacy_laws_report_2024_session_overview.pdf.

[29] Lothar Determann, California Privacy Law – Practical Guide and Commentary, U.S. and State Privacy Law, 5th Ed. (2023), Ch. 2 C and F. Some other state consumer privacy laws may exempt GLBA-regulated financial institutions (including their affiliates) more broadly. *See, e.g.*, Colo. Rev. Stat. § 6-1-1304(2)(j)(II).

[30] Lothar Determann, Brian Hengesbaugh & Avi Toltzis, *American Privacy Rights Act - a first glance at the US Congress's newest comprehensive privacy bill*, 6 Journal of Data Protection & Privacy, 375 (2024).

[31] Cal. Civ. Code §§ 1798.29, 1798.82.

[32] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, www.occ.gov/news-issuances/news-releases/2005/nr-ia-2005-35a.pdf.

[33] 6 U.S.C. §§ 681- 681g.

[34] 6 U.S.C. § 652.

[35] Standards for Safeguarding Customer Information, 16 C.F.R. § 314 (2024), https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314.

[36] 16 C.F.R. § 314.1(a) (2024).

[37] 23 NYCRR Part 500, https://www.dfs.ny.gov/system/files/documents/2023/12/rf23_nycrr_part_500_amend02_20231101.pdf.

requirements for large entities, known as "Class A companies."[38] Additionally, in 2023 the Securities and Exchange Commission ("SEC") adopted new rules to enhance disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934.[39] Under the SEC's Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure[40] regulated entities are required to report cybersecurity incidents within four days and include details of their cybersecurity processes into their annual reports.[41] Some financial institutions are subject to additional layers of SEC data regulation; for example, the SEC's Regulation S-P requires broker-dealers, investment companies, and investment advisers to adopt written incident response policies and to notify their customers of incidents involving unauthorized access to their data, among other requirements.[42] In 2021, President Biden issued an Executive Order on Improving the Nation's Cybersecurity.[43]

Concerning artificial intelligence, U.S. legislatures are initially taking a similar harm-specific approach as they have been taking with respect to data privacy. In 2018, California enacted a "bot disclosure law," effective since July 2019, under which online service providers must disclose the deployment of AI tools for online chats to prevent misleading consumers about whether they are communicating with a human or a machine.[44] Utah enacted similar disclosure obligations in the Utah Artificial Intelligence Policy Act, which took effect in May 2024.[45]

After news stories broke in 2018 that developers noticed gender discrimination caused by AI-based recruitment tools, lawmakers began focusing on bias prevention.[46] Since January 2023, a City of New York ordinance has regulated "automated employment decision tools".[47] Employers in New York City that use such tools are required to conduct annual bias audits, disclose audit results publicly, and inform candidates and employees that automated employment decision tools will be used and allow them to request alternative evaluation processes.[48] In August 2024, Illinois passed a law amending the Illinois Human Rights Act under which employers are subject to civil rights claims if they use AI tools in hiring and other employment decisions and cause discrimination.[49] Employers will be required to notify employees whenever they use AI tools with respect to the "recruitment, hiring, promotion, renewal of employment, selection for training or apprenticeship, discharge, discipline, tenure, or the terms, privileges, or conditions of employment."[50] The amended law applies to discrimination based on the list of protected classes under Illinois law, as well as using "zip codes as a proxy for protected classes."[51] The changes in law are set to take effect Jan. 1, 2026. Likewise, although with a broader scope and not only limited to employment cases, the State of Colorado passed a bill ("Colorado AI Act"[52]), aiming to prevent algorithmic discrimination caused by high-risk artificial intelligence systems, which takes effect on February 1, 2026. The law considers decisions in certain areas, such as employment, financial, services, and health care, to be "consequential", thus labeling AI systems that make such decisions or are a substantial factor in decision

[38] 23 NYCRR Part 500, Sec. 500.1(d).

[39] 15 U.S.C. § 78a seqq.

[40] 17 C.F.R. §§ 229, 232, 239, 240, and 249, https://www.govinfo.gov/content/pkg/FR-2023-08-04/pdf/2023-16194.pdf.

[41] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51896, 51924 (August 4, 2023).

[42] 17 C.F.R. §§ 270-75.

[43] Executive Order 14028 – Improving the Nation's Cybersecurity, 86 Fed. Reg. 26633 (May 12, 2021) https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf.

[44] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001.

[45] https://le.utah.gov/~2024/bills/sbillenr/SB0149.pdf.

[46] Jeffrey Dastin, *Insight - Amazon scraps secret AI recruiting tool that showed bias against women*, Reuters, October 10, 2018, https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/.

[47] Automated employment decision tools, N.Y.C. Local Law No. 144 (N.Y.C. 2021).

[48] R.C.N.Y. § 5-301 seqq.

[49] House Bill 3773, *see* https://ilga.gov/legislation/103/HB/PDF/10300HB3773lv.pdf.

[50] 775 ILCS 5/2-102(L)(1).

[51] 775 ILCS 5/2-102(L)(1).

[52] Concerning Consumer Protections in Interactions with Artificial Intelligence Systems, Col. Assemb. B. 24-205 (Col. Stat. 2024).

making "high-risk systems".[53] In consequence, deployers and developers are subject to a multitude of reporting, documentation, transparency, and risk assessment requirements.[54]

California also enacted more than a dozen new AI-specific laws on concrete topics, including: AB 2013 (Generative artificial intelligence: training data transparency), requiring developers of generative AI systems to publicly disclose information about the datasets used to train their models;[55] SB 942 (California AI Transparency Act), requiring large AI developers to include watermarks for AI-generated content as well as provide tools for users to identify such content;[56] AB 3030 (Health care services: artificial intelligence) requiring healthcare providers to disclose AI-generated patient communications that involve clinic information;[57] SB 1120 (Health care coverage: utilization review) prohibiting health plans and insurers from using AI or other algorithms to supplant health care provider decision-making.[58] Three new California laws target AI-generated or -manipulated pornography.[59] Two new California laws target AI-generated misinformation,[60] which were enjoined by a court on freedom-of-speech grounds a few days after the California governor signed the bills into law in September 2024.[61] On September 29, 2024, California Governor Gavin Newsom vetoed a broader AI safety bill,[62] the Secure Innovation for Frontier Artificial Intelligence Models Act,[63] which would have exposed the industry to considerable obligations and liability risks, supervised by a newly established authority. Governor Newsom noted in his veto decision that California is home to 32 of the world's top 50 AI companies and therefore particularly obligated to prevent harms from AI, but also that the concrete sector-, situation-, and harm-specific laws that he had signed the previous weeks were enough initially and that the vetoed bill was overbroad and detrimental to innovation.[64]

As U.S. broker-dealers and SEC-registered investment advisers ("RIAs") use AI systems more frequently, the SEC and Financial Industry Regulatory Authority, Inc. ("FINRA") have devoted more attention to this issue as well.[65] Recent regulatory developments underscore the SEC's heightened focus on addressing conflicts of interest through stricter oversight, including Proposed SEC Rules, which require firms to neutralize biases in their algorithms and aim to address conflicts of interest that could emerge from the use of predictive data analytics and related technologies – including AI – by RIAs or broker-dealers, potentially prioritizing the firms' interests over those of their investors.[66] Likewise, FINRA's 2020 report on Artificial Intelligence in the Securities Industry[67] consolidates multiple AI-related FINRA rules into a comprehensive framework, creating a roadmap for key compliance considerations, including

[53] Colo. Rev. Stat. § 6-1-1701 (2) seqq.

[54] Colo. Rev. Stat. § 6-1-1702 seqq.

[55] Cal. Assemb. B. 2013, Chapter 817 (Cal. Stat. 2024).

[56] Cal. S. B. 942, Chapter 291 (Cal. Stat. 2024).

[57] Cal. Assemb. B. 3030, Chapter 848 (Cal. Stat. 2024).

[58] Cal. S. B. 1120, Chapter 879 (Cal. Stat. 2024).

[59] SB 1381 (Crimes: child pornography) prohibits sexually explicit deepfakes (including depicting children); SB 926 (Crimes: distribution of intimate images) criminalizes the intentional creation and distribution of sexually explicit deepfake images of identifiable persons with intent to cause serious emotional distress; SB 981 (Sexually explicit digital images) requires social media platforms to create mechanisms for reporting and taking down sexually explicit deepfakes.

[60] AB 2655 (Defending Democracy from Deepfake Deception Act of 2024) requires online platforms with over 1 million California users to remove or label inauthentic, fake, or false content related to elections during the months leading up to, and after, an election, within three days of a user reporting it; AB 2839 (Elections: deceptive media in advertisements) prohibits the knowing distribution of election materials or advertisements with materially deceptive content – unless the content is labeled as having "been manipulated for purposes of satire or parody."

[61] *Kohls v. Bonta*, Docket No. 2:24-cv-02527 (E.D. Cal. Oct 2, 2024).

[62] Veto-Message: S.B. 1047, September 29, 2024, https://www.gov.ca.gov/wp-content/uploads/2024/09/SB-1047-Veto-Message.pdf.

[63] Secure Innovation for Frontier Artificial Intelligence Models Act, Cal. S.B. 1047.

[64] Veto-Message: S.B. 1047, September 29, 2024, https://www.gov.ca.gov/wp-content/uploads/2024/09/SB-1047-Veto-Message.pdf.

[65] Jennifer D. Morton, *The Use of AI in the Securities Industry: U.S. Regulatory Considerations for Broker-Dealers and SEC-Registered Investment Advisers*, 57 The Review of Securities & Commodities Regulation 19 (2024).

[66] Rel No. 34-97990 (2023) at 42, *text available at*: https://www.sec.gov/files/rules/proposed/2023/34-97990.pdf.

[67] Artificial Intelligence ("AI") in the Securities Industry, FINRA, (June 2020), *text available at*: https://www.finra.org/sites/default/files/2020-06/ai-report-061020.pdf.

updating model risk management, mitigating data bias, protecting client information, ensuring the suitability of AI-driven recommendations, addressing cybersecurity risks, and maintaining transparent and compliant communication.[68]

Businesses within and outside the financial sector should analyze each of these new laws to determine whether they are covered or exempt, and what concrete compliance measures are required. Given the specificity of U.S. laws, businesses tend to find it relatively easy to determine the applicable requirements. But, they suffer greatly from the sheer volume of new U.S. laws.

IV. EU COMPLIANCE CHALLENGES IN NIS2, DORA, AND THE AI ACT

Turning to specific technology and AI regulation in the EU, businesses find relatively fewer, but much more lengthy, complex, and principle-based regulations. For example, the NIS 2 Directive,[69] DORA,[70] and the AI Act[71] contain numerous provisions that financial sector businesses must analyze and address.

1. NIS 2 Directive

Many companies in the financial sector should already be familiar with national laws that implemented the network infrastructure security requirements of the NIS Directive from 2016,[72] because it applied to certain financial sector entities as "operators of essential services."[73] On January 16, 2023, a successor directive entered into force – Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, the so-called "NIS 2 Directive" (or simply "NIS 2").[74] The European Union addresses directives, like NIS 2, to the member states of the EU or the broader European Economic Area ("EEA"),[75] which are required to transpose its rules into national law. Companies need to comply with those implementing national laws, not typically the directive directly. EU Member States were required to transpose the rules of the NIS 2 Directive into national law by October 17, 2024; however, only a few EU member states met this deadline.[76]

In the NIS 2 Directive, the EU prescribes technical, organizational, and administrative data security measures that entities must implement to achieve a high common level of cybersecurity across the EEA.[77] Member states are free to enact stricter laws, requiring a higher level of security, which may result in differences in national laws.[78] The NIS 2 Directive extends the scope of its predecessor's requirements in several ways, covering additional sectors and businesses and adding substantive requirements that apply to covered businesses.

---

[68] Jennifer D. Morton, *The Use of AI in the Securities Industry: U.S. Regulatory Considerations for Broker-Dealers and SEC-Registered Investment Advisers*, at 204, 57 *The Review of Securities & Commodities Regulation* 19, at 204 (2024).

[69] Directive (EU) 2022/2555 of the European Parliament and the Council of 14 December 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 Directive (EU) 2016/1148 (NIS 2 Directive), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555.

[70] Regulation 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554.

[71] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized 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 (Artificial Intelligence Act), *text available at* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689.

[72] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148.

[73] Art. 4(4) NIS Directive.

[74] Directive (EU) 2022/2555 of the European Parliament and the Council of 14 December 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 Directive (EU) 2016/1148 (NIS 2 Directive), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555.

[75] Which includes also Iceland, Liechtenstein, and Norway.

[76] Among them Belgium, Croatia, and Hungary, *see* Rachel de Souza, *EU: NIS2 Member State Implementation Deadline Has Arrived*, https://www.jdsupra.com/legalnews/eu-nis2-member-state-implementation-4271351.

[77] Art. 1(1) NIS 2 Directive.

[78] Art. 5 NIS 2 Directive.

a. Scope of application

Companies in the financial sector are covered by the NIS 2 Directive, if they: (1) qualify as a particular type of entity in the "sectors of high criticality" (Annex I of the NIS 2 Directive) or "other critical sectors" (Annex II of the NIS 2 Directive); (2) are at least so-called medium-sized enterprises within the meaning of EU Recommendation 2003/361/EC,[79] *i.e.* (i) employ at least 50 persons and/or (ii) have an annual turnover of at least EUR 10 million or an annual balance sheet total of at least EUR 10 million; and (3) provide their services in the Union or carry out their activities there.[80]

Businesses can find lists of covered sectors, subsectors, and entities in NIS 2's Annexes. Of particular relevance is Annex I of the NIS 2 Directive, which lists in No. 3 "banking" and in No. 4 "financial market infrastructure" as sectors. The sector "banking" covers "credit institutions as defined in Article 4, point (1), of Regulation (EU) No. 575/2013" (*i.e.* an "undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account"), "financial market infrastructures" covers "operators of trading venues as defined in Article 4, point (24), of Directive 2014/65/EU" and "central counterparties ("CCPs") as defined in Article 2, point (1), of Regulation (EU) No. 648/2012."[81]

Additionally, companies in the financial sector should check whether they are covered by the NIS 2 Directive due to another reason, *e.g.*, because they provide ICT service management,[82] or they are covered regardless of their size, *e.g.*, because they are identified as critical entities under Directive (EU) 2022/2557[83] and national implementation laws. The NIS 2 Directive differentiates between essential and important entities[84] concerning supervision and enforcement measures.

b. Obligations

Under the NIS 2 Directive, businesses need to satisfy numerous obligations, including:

i. ***Cybersecurity risk-management-measure implementation.***[85] Businesses must take appropriate and proportionate technical, operational, and organizational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimize the impact of incidents on recipients of their services and on other services. The measures must in particular take into account the state-of-the-art and shall ensure a level of security of network and information systems appropriate to the risks posed. The NIS 2 Directive lists some minimum requirements for those measures.

ii. ***Governance requirements.***[86] Management bodies of covered entities must approve the cybersecurity risk-management measures taken, oversee their implementation, and can be held liable for infringements by the entities. Further, members of the management bodies are required to follow training and shall encourage covered entities to offer similar training to their employees on a regular basis.

iii. ***Registration obligations.***[87] Businesses must register with authorities in jurisdictions where they are established. Companies that are not established in any EEA member state and do not designate a representative in the EU, and companies that provide certain types of

[79] Commission Recommendation of 6 May 2003 concerning the definition of micro-, small-, and medium-sized enterprises, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF.

[80] Art. 2(1) NIS 2 Directive; *see* Stefan Hessel, Christoph Callewaert and Moritz Schneider, *Die NIS-2-Richtlinie aus Unternehmensperspektive [The NIS-2 Directive from a business perspective]*, RDi 2024, 208, 210.

[81] Annex I No. 3 and 4 of the NIS 2 Directive.

[82] Managed Service Providers are defined in Art. 6 No. 39 NIS 2 Directive as "an entity that provides services related to the installation, management, operation, or maintenance of ICT products, networks, infrastructure, applications, or any other network and information systems, via assistance or active administration carried out either on customers' premises or remotely."

[83] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557. Art. 2(3) NIS 2 Directive.

[84] Art. 3 NIS 2 Directive.

[85] Art. 21 NIS 2 Directive.

[86] Art. 20 NIS 2 Directive.

[87] Art. 3(4) and 27 NIS 2 Directive.

telecommunications services, may be required to register with authorities in every jurisdiction where they provide their services,[88] *i.e.*, potentially in every EEA member state separately, with forms in local languages.

iv. ***Reporting obligations.***[89] Businesses are required to notify authorities of significant incidents without undue delay, subject to a multi-stage reporting process, beginning with a requirement to submit early warnings within 24 hours. The NIS 2 Directive also requires reporting to customers concerning significant incidents that are likely to adversely affect them. Further, it foresees an information requirement concerning any significant cyber threat to the recipients of their services that are potentially affected.

To comply with these reporting obligations, companies must set up processes in advance and align these with reporting and notification processes under other laws, including the GDPR,[90] which requires notifications of personal data breaches to data protection authorities and data subjects. Companies will find that incidents that trigger notification obligations under the NIS 2 Directive will often also trigger notification obligations under the GDPR. According to the GDPR, companies face a "personal data breach" in case of any "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."[91] Under Art 33 GDPR, companies have to notify authorities "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons." Under NIS 2, companies have to notify incidents as significant not only if the incident "has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned" but also if it "has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage."[92] A U.S.-based company subject to NIS 2 and the GDPR may have to notify more than 60 different authorities in the EU alone, given that member states may task different authorities with receiving reports under each law – Germany alone has created 16 data protection authorities. Given the short reporting deadlines – 72 hours under the GDPR and 24 hours under NIS 2 – and varying forms, language requirements, and disclosure obligations under national laws and administrative procedures, companies face impossible tasks in the event of cyber incidents.

c. Relationship to other EU digital regulations

EU lawmakers did not comprehensively align NIS 2 requirements with other laws and regulations. For example, companies may need to notify data protection authorities separately of personal data breaches under the GDPR and significant incidents under NIS 2. Nonetheless, regarding its interplay with sector-specific laws, the NIS 2 Directive stipulates: "Where sector-specific Union legal acts require essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement laid down in Chapter VII, shall not apply to such entities."[93] One sector-specific law applicable to financial entities is the Digital Operational Resilience Act ("DORA").[94] Even though EU lawmakers did not specifically reference DORA by name in the NIS 2 Directive, DORA stipulates that, "in relation to financial entities identified as essential or important entities pursuant to national rules transposing Article 3 of Directive (EU) 2022/2555, this Regulation shall be considered a sector-specific Union legal act for the purposes of Article 4 of that Directive."[95] Thus, financial entities regulated by DORA may not be required to comply with the cybersecurity risk-management measures and incident notification

[88] Art. 26 NIS 2 Directive.

[89] Art. 23 NIS 2 Directive.

[90] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[91] Art. 4(12) GDPR.

[92] Art. 23(3) NIS 2 Directive.

[93] Art. 4(1) NIS 2 Directive.

[94] Regulation 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554.

[95] Art. 1(2) DORA. According to the German Federal Financial Supervisory Authority DORA supersedes the NIS 2 requirements regarding cybersecurity risk-management measures and notification of significant incidents, https://www.bafin.de/SharedDocs/FAQs/DE/DORA/DORA_Landingpage/12.html.

requirements of the NIS 2 Directive.[96] But, they have to assess whether they fall under NIS 2 and/or DORA and to what extent compliance with DORA addresses requirements under NIS 2.

2. DORA

EU lawmakers enacted DORA in the form of a regulation, which entered into force on January 16, 2023 and started to apply after a two-year transition period, since January 17, 2025. Unlike the NIS 2 Directive, which member states must transpose into national laws, DORA applies directly to covered companies. DORA aims to achieve a high common level of digital operational resilience and requires financial sector businesses to implement measures safeguarding the security of network and information systems.[97]

a. Scope of application

Financial entities subject to DORA's definitions and requirements include credit institutions, payment institutions, account information service providers, electronic money institutions, investment firms, crypto-asset service providers and issuers of asset-referenced tokens, central securities depositories, central counterparties, trading venues, trade repositories, managers of alternative investment funds, management companies, data reporting service providers, insurance and reinsurance undertakings, insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, institutions for occupational retirement provision, credit rating agencies, administrators of critical benchmarks, crowdfunding service providers, and securitization repositories.[98] Some companies on the list may not have expected to be regulated as a "financial entity," such as data reporting service providers and credit rating agencies.

DORA also may affect service providers to financial entities, since DORA also applies to so-called ICT third-party service providers.[99] ICT stands for "information and communication technology"[100] and ICT services are defined as "digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware services as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analog telephone services."[101] DORA does not further specify or break down which types of services constitute ICT services, and in a recital, the law stipulates that "the definition of ICT services in the context of this Regulation should be understood in a broad manner, encompassing digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis."[102]

b. Obligations for financial entities

DORA subjects financial entities to a broad range and comprehensive obligations, resulting in a major operational impact. In light of practical differences between types and sizes of financial entities, Art. 4 DORA explicitly stipulates a proportionality principle, under which businesses should consider their size and overall risk profile as well as the nature, scale, and complexity of their services, activities, and operations, as they implement the obligations prescribed by DORA. The EU Commission is to adopt more precise rules and regulations, in the form of delegated and implementing acts to specify how financial entities shall comply with obligations under DORA.[103] On a very high level, to provide an overview, the obligations include in particular:

— **Governance obligations**. Financial entities are required to implement an internal governance and control framework that ensures an effective and prudent management of ICT risk in order to achieve a high level of digital operational resilience.[104] The management body of the financial entity shall bear the ultimate responsibility for managing the financial entity's ICT risks,[105] bear the overall

[96] cf. also Communication from the Commission: Commission Guidelines on the application of Article 4(1) and (2) of Directive (EU) 2022/2555 (NIS 2 Directive) (2023/C 328/02), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023XC0918(01).

[97] Art. 1(1) DORA.

[98] Art. 2(1) lit. a-t DORA. DORA also foresees a few exceptions.

[99] Art. 2(1) lit. u DORA.

[100] Recital 1 DORA.

[101] Art. 3 No. 21 DORA.

[102] Recital 35 DORA.

[103] https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en.

[104] Art. 5(1) DORA.

[105] Art. 5(2) lit. a DORA.

responsibility for setting and approving the digital operational resilience strategy,[106] and shall define, approve, oversee, and be responsible for the implementation of all arrangements related to the ICT risk-management framework referred to in Art. 6 DORA.[107] Management shall take various measures, including putting in place policies that aim to ensure the maintenance of a high standard of availability, authenticity, integrity, and confidentiality of data, setting clear roles and responsibilities for ICT-related functions, and establishing appropriate governance arrangements to ensure effective and timely communication, cooperation, and coordination among these functions. Another management obligation is to implement reporting channels at corporate levels that enable it to be duly informed regarding ICT service providers (*e.g.*, agreements with ICT service providers, any relevant planned material changes regarding the ICT service providers, and the potential impact of such changes).[108] Managers are also required to keep up to date with sufficient knowledge and skills, including specific training on a regular basis.[109]

— **ICT risk-management obligations**. Under DORA, financial entities shall have a sound, comprehensive, and well-documented ICT risk-management framework that is part of their overall risk-management system.[110] This should enable them to address ICT risks quickly, efficiently, and comprehensively and to ensure a high level of digital operational resilience. The ICT risk-management framework shall include at least strategies, policies, procedures, as well as ICT protocols and tools that are necessary to duly and adequately protect all information assets and ICT assets (including software, hardware, and servers), as well as to protect relevant physical components and infrastructure in order to ensure the adequate protection of all information assets and ICT assets from risks, including damage and unauthorized access or usage.[111]

— **Incident management and reporting**. Under DORA, financial entities are required to define, establish, and implement an ICT-related incident management process to detect, manage, and notify ICT-related incidents.[112] First, financial entities must record all ICT-related incidents and significant cyber threats, and establish appropriate procedures and processes to ensure, in particular, the monitoring, handling, and follow-up of ICT-related incidents and to prevent the occurrence of such incidents.[113] Furthermore, financial entities shall classify ICT-related incidents and determine their impact based on certain criteria, *e.g.*, number of clients affected, duration of the ICT-related incident, geographical spread, criticality of the services affected, and economic impact.[114] Major ICT-related incidents shall generally be reported by financial entities to the competent authority pursuant to Art. 46 DORA.[115]

An "ICT-related incident" is defined as "a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity, or confidentiality of data, or on the services provided by the financial entity."[116] A "major ICT-related incident" is defined as "an ICT-related incident that has a high adverse impact on the network and information systems that support critical or

[106] Art. 5(2) lit. d DORA.

[107] Art. 5(2) DORA.

[108] Art. 5(2) lit. i DORA.

[109] Art. 5(4) DORA.

[110] Art. 6(1) DORA.

[111] Art. 6(2) DORA.

[112] Art. 17(1) DORA

[113] Art. 17(2) DORA.

[114] Art. 18(1) DORA. The Delegated Regulation (EU) 2024/1772 specifies the criteria for classification of ICT-related incidents and cyber threats, *see* Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401772.

[115] Art. 19(1) DORA.

[116] Art. 3 No. 8 DORA.

important functions of the financial entity."[117] The Delegated Regulation (EU) 2024/1772 provides further guidance for companies on when an incident shall be considered a major incident and sets out materiality thresholds.

Regarding the reporting to the authorities, financial entities are subject to a multi-stage reporting process under DORA, comprising an initial notification, an intermediate report, and a final report.[118] DORA contemplates that deadlines and contents for notifications will be prescribed in a separate act that will require initial reports to be submitted within 24 hours.[119]

If a major ICT-related incident occurs that has an impact on the financial interests of clients, financial entities shall, without undue delay, inform their clients as soon as they become aware of it, about the major ICT-related incident and of the measures that have been taken to mitigate the adverse effects of such incident.[120] Significant cyber threats may be notified, on a voluntary basis, to the relevant competent authority if financial entities are of the opinion that the threat is relevant to the financial system, service users, or clients.[121] "Cyber threat" is defined as "any potential circumstance, event, or action that could damage, disrupt, or otherwise adversely impact network and information systems, the users of such systems, and other persons."[122] A "significant cyber threat" means "a cyber threat the technical characteristics of which indicate that it could have the potential to result in a major ICT-related incident or a major operational or security payment-related incident."[123]

— **Regular digital operational resilience testing obligation**. Financial entities covered under DORA that are not microenterprises shall also establish, maintain, and review a comprehensive digital operational resilience testing program as an integral part of the risk-management framework, taking into account the proportionality principle.[124] When designing and implementing the program, financial entities shall apply a risk-based approach.[125]

— **ICT third-party, risk-management obligation**. Additionally, financial entities must satisfy DORA's ICT third-party, risk-management requirements, which shall be managed as an integral component of ICT risk within their ICT risk-management framework in accordance with certain principles.[126] For example, financial entities that have in place contractual arrangements for the use of ICT services to run their business operations, should remain, at all times, fully responsible for the compliance with and the fulfillment of the obligations of DORA and applicable financial services law.[127]

Financial entities must maintain a register of information in relation to all contractual arrangements on the use of ICT services provided by third-party ICT service providers and update this register of information.[128] Also, financial entities must report at least yearly to the competent authorities on the number of new arrangements on the use of ICT services, the categories of ICT service providers, the type of contractual arrangements, and the ICT services and functions that are being provided.[129]

Before financial entities conclude contracts with service providers, they are obligated to conduct

[117] Art. 3 No. 10 DORA.

[118] Art. 19(4) DORA.

[119] Art. 20 DORA. Commission Delegated Regulation of October 23, 2024 supplementing Regulation (EU) 2022/2554 with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats (however, not in force until published in the Official Journal).

[120] Art. 19(3) DORA.

[121] Art. 19(2) DORA.

[122] Art. 3 No. 12 DORA in connection with Art. 2 No. 8 Cybersecurity Act (Regulation (EU) 2019/881).

[123] Art. 3 No. 13 DORA.

[124] Art. 24(1) DORA.

[125] Art. 24(3) DORA.

[126] Art. 28(1) DORA.

[127] Art. 28(1) lit. a DORA.

[128] Art. 28(3) DORA.

[129] Art. 28(3) DORA.

certain analyses, including identifying and assessing all relevant risks in relation to the contractual arrangement.[130] Furthermore, financial entities must abide by certain requirements regarding agreements on the use of ICT services. In formal terms, the contract must be set out in writing and must be available to the parties on paper, or in a document with another downloadable, durable, and accessible format.[131] Content-wise, the contract must clearly allocate the rights and obligations of the financial entity and of the ICT service provider, and include at least the elements listed in Art. 30 (2) DORA. These elements cover a broad range and requirements that contracts must include, for example, a clear and complete description of all functions and ICT services to be provided by the ICT service provider, indicating whether and under which conditions subcontracting is permitted,[132] as well as provisions on availability, authenticity, integrity, and confidentiality in relation to the protection of data, including personal data.[133] They must also include termination rights and related minimum notice periods for the termination.[134] If the ICT services support critical or important functions, additional contractual elements are required.[135] Financial entities may have to also update existing agreements[136] and should provide service providers sufficient lead time, given that these will likely face a surge in requests from all customers impacted by DORA.[137]

EEA-based financial entities that work with service providers outside the EEA need to also address data protection law requirements for international data transfers.[138] With respect to service providers in the United States, financial entities in the EEA may be able to rely on the EU-U.S. Data Privacy Framework,[139] but should also consider signing contracts including the EU Standard Contractual Clauses.[140]

— **Impact on ICT service providers contracting with financial entities**. Financial entities subject to DORA's requirements should distinguish between "general" ICT service providers and "critical" ICT service providers that are directly supervised. The designation of ICT service providers that are critical to financial entities as "critical ICT third-party service providers" is carried out by the European Supervisory Authorities[141] on the basis of certain criteria, such as the systemic impact on the stability, continuity, or quality of the provision of financial services, the reliance of financial entities on the services of the relevant ICT service provider with regard to critical or

[130] Art. 28(4) lit. c DORA.

[131] Art. 30(1) DORA.

[132] Art. 30(2) lit. a DORA.

[133] Art. 30(2) lit. c DORA.

[134] Art. 30(2) lit. h DORA.

[135] Art. 30(3) DORA. In this context, please *also see* Commission Delegated Regulation 2024/1773 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401773.

[136] Recital 69 DORA.

[137] Thorsten Ammann und Yannick Zirnstein, *DORA – IT-Sicherheit gesetzlich verordnet [DORA - IT security decreed by law]*, CB 2023, 21, 26.

[138] Art. 29(2) DORA.

[139] Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj; *see* Lothar Determann, Michaela Nebel and Michael Schmidl, The EU-US data privacy framework and the impact on companies in the EEA and USA compared to other international data transfer mechanisms, Journal of Data Protection and Privacy 120 (2024).

[140] Thomas Kahl and Charlotte Dreisigacker-Sartor, *DORA, internationaler Datentransfer und der neue EU-US Datenschutzrahmen [DORA, international data transfer and the "new" EU-US data protection framework]*, CB 2023, 436, 439 seq.; Lothar Determann, Holger Lutz, Michaela Nebel, International Data Transfer and Trade Restraints, CRi 2022, 140.

[141] *i.e.*, the EBA, ESMA, EIOPA.

important functions of financial entities, and the degree of substitutability of the ICT service provider.[142]

General ICT service providers are indirectly affected by DORA as well. Even if they do not specifically target prospective customers in the financial sector, they will likely try to contract with financial institutions, who will need to request changes to standard contract terms in order to meet DORA requirements. Critical ICT service providers are even more directly affected, because they will become subject to direct supervision by regulators enforcing DORA going forward.

3. Other EU Cybersecurity Laws

There are also other laws that companies in the financial sector must consider in the context of cybersecurity. For example, another proposal that has just recently been published in the Official Journal of the EU is the Cyber Resilience Act, which contains cybersecurity requirements for products with digital elements.[143]

4. EU AI Act

After a three-year-long legislative process and numerous revisions and controversial debates, the EU finally enacted its AI Act effective August 1, 2024.[144] Companies are granted transition periods and become subject to several different compliance deadlines in 2025, 2026, and 2027.[145] With the AI Act, EU lawmakers sought "to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence ("AI"), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law, and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation."[146] Companies must comply with the AI Act in addition to all existing laws and regulations, including the GDPR, which already regulates automated decision-making to protect "rights and freedoms" of individuals and which continues to apply.[147]

a. Scope of application

The AI Act lays down rules for AI systems and for general-purpose AI models. The term "AI system" is defined as "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs, such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."[148] The term "general-purpose AI models" is defined as an "AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development, or prototyping activities before they are placed on the market."[149] The AI Act

---

[142] The Commission Delegated Regulation (EU) 2024/1502 of 22 February 2024 specifies the criteria for the designation of ICT third-party service providers as critical for financial entities; Commission Delegated Regulation (EU) 2024/1502 of 22 February 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council by specifying the criteria for the designation of ICT third-party service providers as critical for financial entities https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401502.

[143] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402847.

[144] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized 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 (Artificial

footnote continued from previous column…

Intelligence Act), text available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689.

[145] Art. 113 AI Act.

[146] Art. 1(1) AI Act.

[147] Lothar Determann and Michaela Nebel, GDPR v. AI Act & Other EU Data Regulation, Bloomberg Law (April 23, 2024), https://www.bloomberglaw.com/external/document/X89VQB00000000/tech-telecom-professional-perspective-gdpr-v-ai-act-other-eu-dat.

[148] Art. 3 No. 1 AI Act.

[149] Art. 3 No. 63 AI Act.

generally applies to all sectors, including companies in the financial industry, which are called out in several articles.[150]

The AI Act applies to providers "placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union, irrespective of whether those providers are established or located within the Union or in a third country."[151] Furthermore, the AI Act applies to "deployers of AI systems that have their place of establishment or are located within the Union,"[152] *i.e.*, business and individual users except "where the AI system is used in the course of a personal non-professional activity."[153]

b. Obligations

With the AI Act, EU lawmakers adopted a risk-based approach and defined categories of prohibited AI systems, high-risk AI systems, other AI systems, and general-purpose AI models. Which obligations apply depends on the risk category and also on whether the company qualifies as a provider or as a deployer.

i. ***Prohibitions***. Certain practices are generally prohibited under Art. 5 AI Act, including, for example, an "AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behavior of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm."

ii. ***High-risk AI Systems***. Not entirely prohibited, but highly regulated, are high-risk AI systems under Art. 6 AI Act (which include safety components of products and products listed on Annexes I) and AI systems referred to on Annex III, such as remote biometric identification systems; AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score; and AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance. Companies can try to document that AI systems listed in Annex III shall not be considered to be high risk where a system does not pose a significant risk of harm to the health, safety, or fundamental rights of natural persons, including by not materially influencing the outcome of decision making (except in case of profiling of natural persons), subject to registration obligations.[154] For example, companies may get comfortable that AI systems used for asset management purposes are arguably unlikely to fall under Article 6, as they typically do not present explicit risks to safety, health, or fundamental rights and are not covered under Annex III of the AI Act.[155] The AI Act provides that the Commission shall provide guidelines specifying the practical implementation together with a comprehensive list of practical examples of use cases of AI systems that are high risk and not high risk, which may contain use cases that will be relevant for the financial industry.[156]

Generally, providers are subject to far more obligations than deployers of high-risk AI systems.[157] They must ensure that these AI systems meet the requirements of Arts. 8 to 15 of the AI Act, concerning risk-management system, data and data governance, technical documentation, record-keeping, transparency, human oversight and the appropriate level of accuracy, robustness, and cybersecurity. With respect to cybersecurity, requirements under the AI Act and DORA overlap, suggesting that companies should align and integrate risk-management measures and documentation

[150] Art. 17(4), Art. 18(3) and recital 158; Art. 2(2)-(12) provide various complex exceptions from applicability.

[151] Art. 2(1) lit. a AI Act.

[152] Art. 2(1) lit. b AI Act.

[153] Art. 3 No. 4 AI Act.

[154] Art. 6(4) AI Act.

[155] Daniel Lühmann and Can Görgülü, *Einsatz von KI im Asset Management [The use of AI in asset management]*, BKR 2024, 175, 178.

[156] Art. 6(5) AI Act.

[157] Art. 16 AI Act stipulates that Art. 8 to 15 must be complied with.

required under Art. 15 of the AI Act and Art. 9(2) of DORA.[158] Furthermore, providers must implement quality management systems, keep certain documentation and logs, and complete or confirm completion of conformity assessments and registrations.[159]

Deployers of high-risk AI systems are also subject to obligations.[160] They shall take appropriate technical and organizational measures to ensure they use such systems in accordance with the instructions for use accompanying the systems. Furthermore, they must assign human oversight to personnel with the necessary competence, training, authority, and support. If they exercise control over the input data, the deployer must ensure that input data are relevant and sufficiently representative in view of the intended purpose of the high-risk AI system. Deployers must monitor the operation of high-risk AI systems on the basis of instructions for use and inform providers and authorities of incidents. Financial institutions may be able to discharge some obligations arising under the AI Act by complying with financial services-specific EU rules on internal governance arrangements, processes, and mechanisms.[161] Deployers must also keep the logs automatically generated by the high-risk AI system, if the logs are under their control,[162] and comply with information requirements (*e.g.*, before deploying high-risk AI systems at the workplace, inform workers' representatives and the affected workers; in case of high-risk AI systems that make decisions or assist in making decisions related to natural persons, deployers must inform the natural persons that are subject to the use of the high-risk AI system). In certain cases, deployers of a high-risk AI system shall perform an assessment of the impact on fundamental rights that the use of such system may produce,[163] including for AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score,[164] and AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance.[165] Once a deployer completes its assessment, it must report the conclusions to authorities via standard forms.[166]

Deployers can also become providers – and thus subject to additional obligations – if they make a substantial modification to a high-risk AI system or if they modify the intended purpose of an AI system, including a general-purpose AI system.[167]

iii. ***Transparency obligations for other AI Systems***. Providers shall ensure that AI systems intended to interact directly with natural persons – for example, when financial sector businesses deploy chatbots to answer customer questions – are designed and developed in such a way that the persons concerned are informed that they are interacting with an AI system.[168] Also, deployers of an AI system that generates or manipulates image, audio, or video content constituting a deep fake – that is, an "AI-generated or manipulated image, audio, or video content that resembles existing persons, objects, places, entities, or events and would falsely appear to a person to be authentic or truthful"[169] – shall disclose that the content has been artificially generated or manipulated.[170]

iv. ***AI literacy obligation***. Irrespective of the risk classification, providers, and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their

[158] René Knoblich and Dieter Krimphove, *Die neue KI-VO im Regelungsdickicht des Aufsichtsrechts [The New AI Regulation in the Regulatory Thicket of Supervisory Law]*, BKR 2024, 843, 845 seq.

[159] Art. 16 seqq. AI Act.

[160] Art. 26 AI Act.

[161] Art. 17(4) AI Act.

[162] Art. 26(6) AI Act.

[163] Art. 27 AI Act.

[164] Annex III point 5 lit. b AI Act.

[165] Annex III point 5 lit. c AI Act.

[166] Art. 27(3) AI Act.

[167] Art. 25 AI Act.

[168] Art. 50(1) AI Act.

[169] Art. 3 No. 60 AI Act.

[170] Art. 50(4) AI Act.

behalf, taking into account their technical knowledge, experience, education, and training, and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.[171] "AI literacy" means "skills, knowledge, and understanding that allow providers, deployers, and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause."[172] Measures will likely include AI training as well as policies.

v. ***Obligations for providers of general-purpose AI models***. Providers of general-purpose AI models must comply with specific requirements set out in Art. 51 seq., such as maintaining up-to-date technical documentation[173] and establishing a program to comply with copyright and related rights.[174] In case of general-purpose AI models with systemic risk additional obligations apply.[175]

c. Checklist.

To approach compliance with the highly complex requirements of the EU AI Act, financial sector businesses could work through task- and checklists, for example, as follows:

i. **Identify and Document AI Systems**. Assess and document which systems used within the company qualify as AI systems or general-purpose models under the EU AI Act, and clarify the company's responsibility role, *e.g.*, provider, deployer, manufacturer, importer, or distributor

ii. **Verify Prohibited AI Systems**. Confirm that no AI systems falling under Art. 5 AI Act are in use, such as systems with certain manipulation potentials and purposes, systems for social scoring, or systems to infer emotions in workplaces

iii. **Identify High-Risk Systems**. For high-risk systems covered by Art. 6 AI Act, ensure:

- suitability of training data
- human oversight
- compliance with monitoring and recording obligations, including after selling systems and products
- security protection and testing (robustness and cybersecurity)
- conformity assessments by designated authorities or certification by specialists, as required, CE marking, and labeling
- documentation is created or reviewed, including for risk and quality management systems, technical and legal dossiers, operating manuals, information for operators, declarations of conformity, CE marking, official registrations, and fundamental rights impact assessments

iv**. Fulfill Transparency Obligations**. Meet transparency requirements for AI systems intended for direct interaction with natural persons, ensuring individuals are aware when they are engaging with AI systems and can recognize artificial generation or manipulation of audio, image, video, or text outputs

v**. Meet Training and Continuing Education Requirements**

vi**. Identify General-Purpose Models**. Before offering general-purpose models:

- Create necessary technical documentation
- Inform companies intending to integrate general-purpose models into AI systems
- Systematically report risks to the EU Commission and implement and document risk assessments and mitigation measures

[171] Art. 4 AI Act.

[172] Art. 3 No. 56 AI Act.

[173] Art. 53(1) lit. a AI Act.

[174] Art. 53(1) lit. c AI Act.

[175] Art. 55 AI Act.

vii. Designate Representatives in the EU (for providers outside the EU)

viii. Report Serious Incidents. Implement procedures for reporting of serious incidents related to high-risk systems to authorities and ensure readiness to cooperate.

If companies fail to comply, they can be subject to severe sanctions from authorities under Articles 99 to 102 of the AI Act. But, the AI Act does not expressly prescribe civil liability. Whether persons harmed by the deployment of AI systems can assert tort claims under national law based on allegations that a company failed to comply with the AI Act depends on national tort laws. Additionally, the EU has published a proposal for a separate AI Liability Directive,[176] which would prescribe specific rules for liability concerning AI systems.[177] Moreover, EU authorities are considering sector-specific rules for AI, including the European Securities and Markets Authority ("ESMA"),which has published a public statement on the use of AI in the provision of retail investment services[178] to provide guidance to investment firms utilizing AI and key obligations under MiFID II,[179] a Directive providing harmonized regulation for investment services. Financial entities have to consider and comply with the AI Act and sector-specific regulatory frameworks.[180]

V. OUTLOOK AND PRACTICAL RECOMMENDATIONS

Financial sector businesses were already subject to a heightened compliance burden as specifically regulated entities for decades. In recent years, they have also become subject to additional technology regulations, as financial institutions create new online offerings and upgrade business processes with technology. On top of sector-specific regulations, financial services businesses increasingly must address technology and AI regulations in their compliance programs, although these regimes are not methodically tailored specifically to financial services companies and thus present different types of compliance challenges, including concerning applicability and compatibility with sector-specific laws.

In order to keep up with the onslaught of technology regulations and operationalize requirements efficiently, businesses need to identify commonalities and differences in regulations and quickly decide which requirements to apply uniformly and globally (based on a "highest-common-denominator" approach) and which requirements to address selectively only for particular jurisdictions, business activities, or situations.

With respect to most data security requirements, for example, companies, including those in the financial sector, should typically adopt the highest required standards and apply them worldwide, given that threats are global, risks can only be managed holistically, and uniformly applied technical, organizational, and administrative data security measures are best suited to reduce risks effectively. Also, even if a particular regulator or legislature has not updated their requirements yet and applies relatively lighter requirements, it is only a question of time until the company can expect to be subjected to new, stricter requirements. Concerning data processing agreements, companies have been piling on new standard contractual clauses developed by additional countries to their global agreements with any service provider anywhere, given that each data privacy and regulatory regime typically requires that financial sector businesses flow through statutory requirements to all service providers worldwide.

By contrast, with respect to documentation and notice requirements, companies will typically need to address specific local requirements concerning content, format, language, and substance of notices. Companies are required by myriad laws to address different topics in registration forms, privacy notices, and security breach notifications – all while keeping notices short and concise. If companies take a "kitchen sink" approach

[176] Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), *text available at*: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0496.

[177] *See* Legislative Observatory of the European Parliament, Procedure File: 2022/0303(COD), https://oeil.secure.europarl.europa.eu/oeil/en/procedure-file?reference=2022/0303(COD).

[178] ESMA, Public Statement On the use of Artificial Intelligence ("AI") in the provision of retail investment services, 30 May 2024, ("ESMA, Public Statement on AI"), text *available at*: https://www.esma.europa.eu/document/public-statement-ai-and-investment-services.

[179] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (MiFID II), text *available at*: https://eur-lex.europa.eu/eli/dir/2014/65/oj/eng.

[180] Petra Buck-Heeb, *MiFID II und der Einsatz von KI [MiFID II and the use of AI]*, BKR 2024, 785, 792.

and try to address multiple disclosure regimes in the same notice document, they may breach mandatory form requirements and inevitably miss required details or violate duties to keep notices short and easy to read.

In between these ends of the spectrum are tasks that benefit from regionalized or hybrid approaches, for example impact assessments. Companies are required to document various assessments under AI laws, data protection laws, cybersecurity laws, and other regulations. The content requirements for impact assessments vary from statute to statute and jurisdiction to jurisdiction, but the risks to be considered show commonalities, including bias, misinformation, and deception under AI laws or identity theft, phishing scams, and fraud under cybersecurity laws. In the interest of efficiency, companies are well advised to first review risks and impacts of new systems, processes, and business plans holistically under all applicable regulatory regimes (confidentially and under attorney-client privilege) and in a second step create locally tailored assessment documentation that they are required to prepare under particular laws and may have to produce to customers, employees, or regulators.

Given the rapid proliferation and change in regulations, companies should actively track updates in legislation, regulations, court decisions, and administrative orders. Also, they need to design compliance programs with regularly scheduled updates. Businesses should be particularly mindful of designing audit controls for their compliance programs in binary, easy-to-determine formats in order to manage the effort required for audits and the effectiveness of following through on remediation measures. Instead of embracing vaguely formulated declarations of good intentions like "company maintains material compliance with all applicable data protection and security laws" or "management ensures responsible and ethical AI usage," companies should adopt audit controls that focus on specific, easily verifiable requirements, *e.g.*, "remote access to all systems requires multi-factor authentication" and "one individual employee is designated as accountable systems steward for every AI system."[181] ■

****

The authors thank Tim Adigüzel for research and editing assistance, but take full responsibility for any errors or omissions. The article reflects the authors' personal opinions and not those of their law firm, clients, or others.

[181] For more practical recommendations on implementing and auditing compliance programs, *see* Determann's Field Guide to Artificial Intelligence Law, Ch. 3 ff. and Determann's Field Guide to Data Privacy Law, Ch. 4 (6th. Ed., forthcoming in January 2025).

The Review of Banking & Financial Services