

MAYER | BROWN

GLOBAL PERSPECTIVES: 2026 CYBERSECURITY AND DATA PRIVACY LANDSCAPE

October 22, 2026

OUR TEAM



PARTNER

ANA BRUDER

FRANKFURT +49 69 7941 1778
ABRUDER@MAYERBROWN.COM



PARTNER

JAD TAHA

DUBAI +971 4 375 7163
JTAHA@MAYERBROWN.COM



PARTNER

AMBER THOMSON

WASHINGTON DC +1 202 263 3456
ATHOMSON@MAYERBROWN.COM



PARTNER

OLIVER YAROS

LONDON +44 20 3130 3698
OYAROS@MAYERBROWN.COM

AGENDA

1. U.S.
2. Middle East
3. Europe: EU and UK
4. Q&A

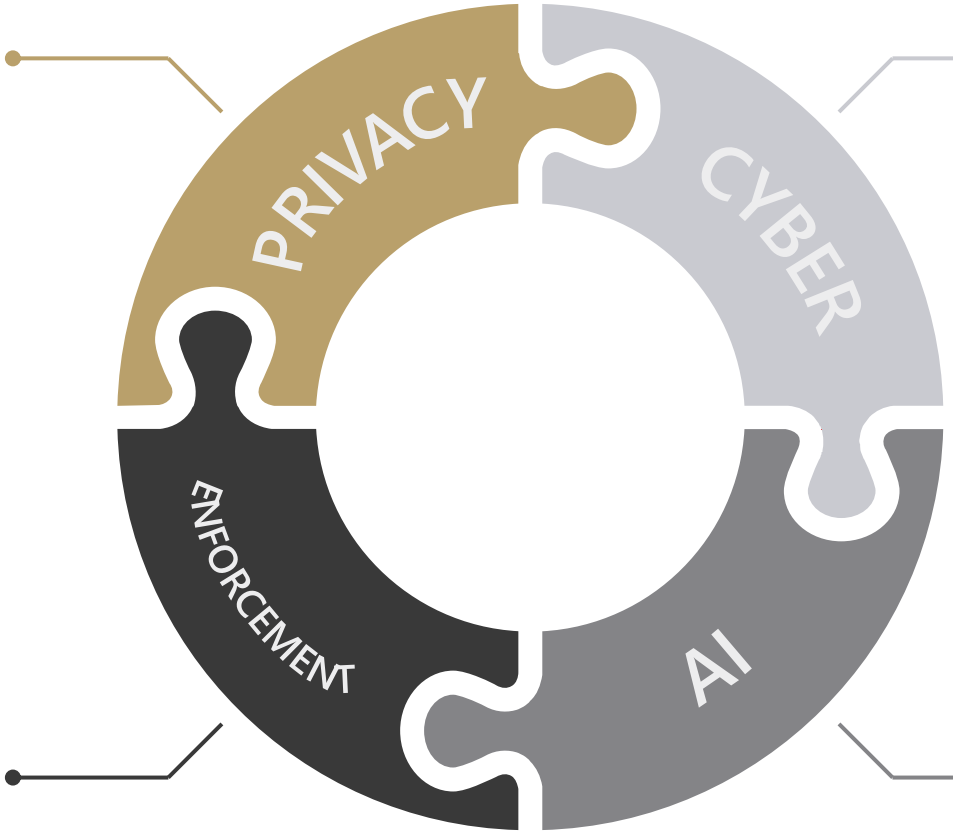

01
U.S.

THE U.S. STORY: FRAGMENTED RULES, HEIGHTENED EXPECTATIONS

The Patchwork

23 enacted state comprehensive privacy laws.

Broad state laws share common architecture, but thresholds, exemptions, and sensitive data rules vary.



Convergence

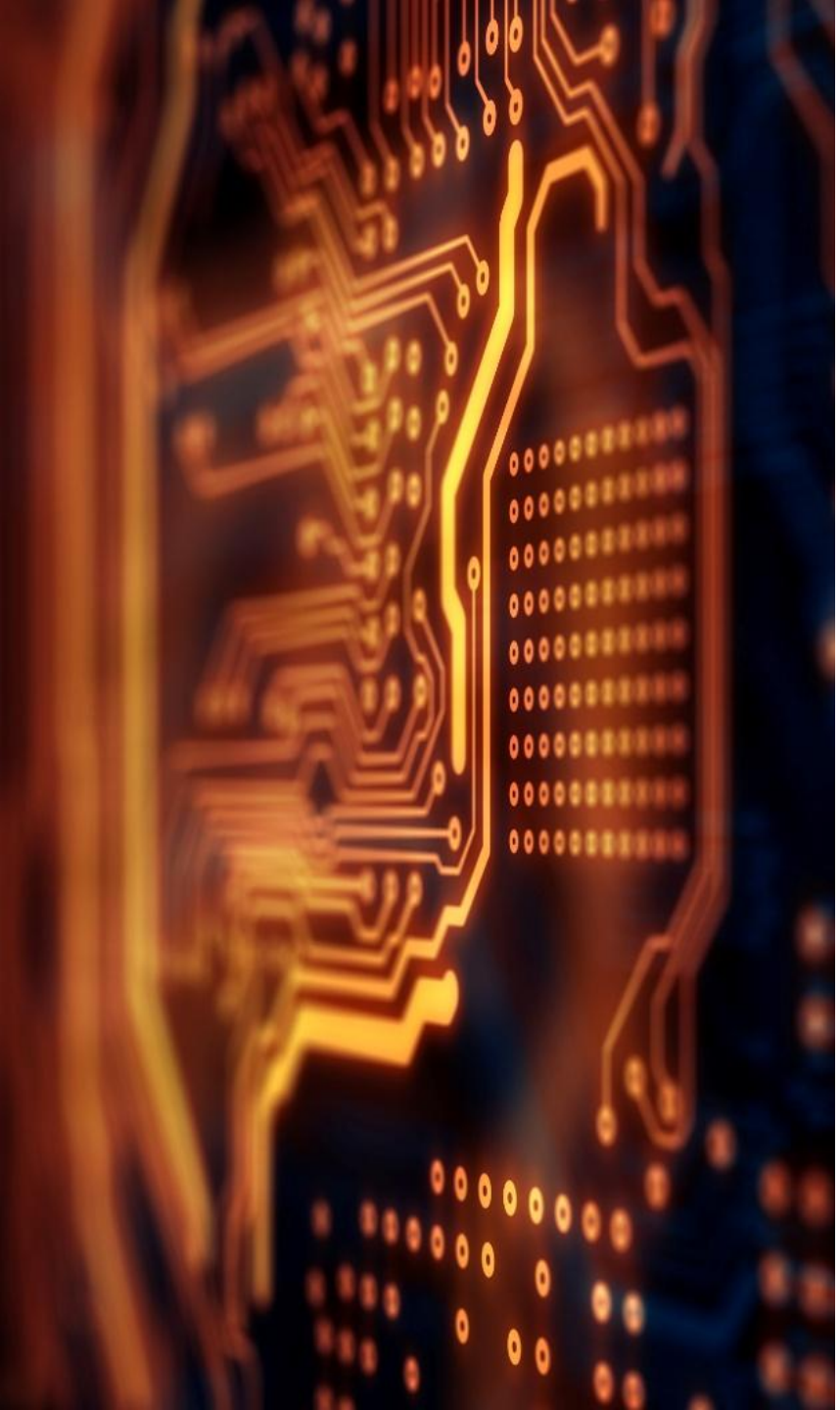
Threats, disclosure duties, and sector rules increasingly converge in incident response.

Heightened Enforcement

Regulators and plaintiffs test whether controls work in practice.

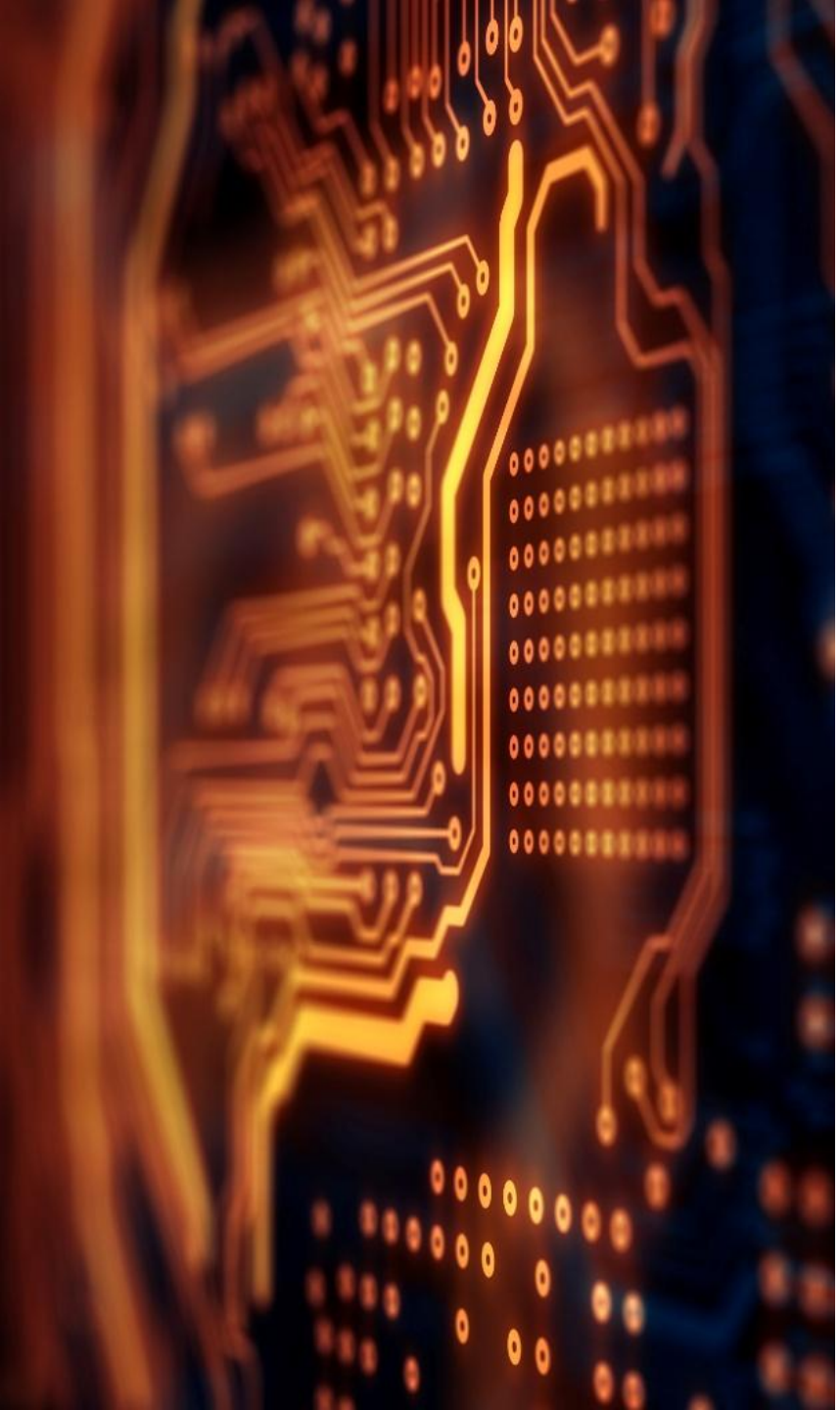
Governance

State laws target consequential decisions, employment tools, consumer interactions and GenAI transparency.



LITIGATION TRENDS PARALLEL TO ENFORCEMENT

- **Private litigation is rising alongside regulatory risk:**
  - Data-breach class actions (even without clear harm)
  - Pixel/SDK tracking lawsuits / CIPA and ECPA lawsuits
  - Biometric privacy litigation
  - AI-related claims (copyright, discrimination, consumer deception)
  - Securities litigation tied to cyber disclosures, breaches
  - Plaintiffs' firms using regulatory findings as litigation roadmaps

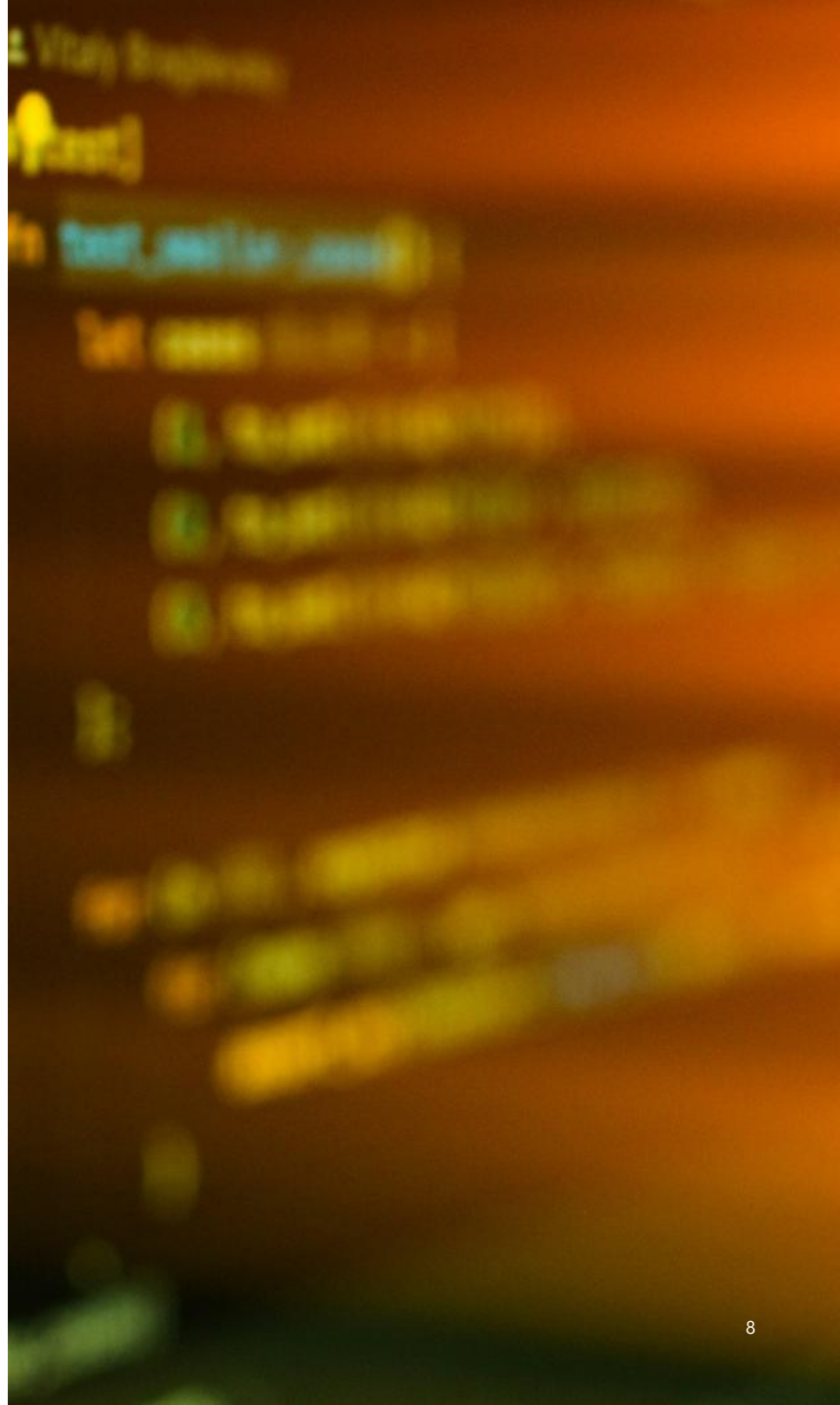


MAJOR UPDATES IN 2026

- CCPA Updates
  - Cybersecurity Audits
  - Risk Assessments
  - ADMT
- Data Broker Law Updates (e.g., California's Delete Act)
- CO AI Act Amendments
- HIPAA Security Rule Update
- Children's Privacy/Security & Social Media Laws
- Executive Order on Advanced AI Innovation and Security
- White House: A National Policy Framework for Artificial Intelligence
- Cyber Strategy for America

TAKEAWAYS

- **More Laws**: More states are enacting privacy laws, while many states are continuing to amend their existing laws.
- **Broader Obligations**: States are also expanding the scope and obligations of their privacy laws, particularly with respect to sensitive data, including children's data.
- **More Enforcement**: Enforcement is increasingly focused on whether privacy compliance works in practice—not just on what companies' policies say.
- **More Litigation**: Private litigation is increasing alongside regulatory enforcement, with plaintiffs' firms increasingly relying on regulatory findings and compliance gaps as roadmaps for class actions and other claims.



ARTIFICIAL INTELLIGENCE & CYBERSECURITY TRENDS



AI-POWERED CYBER THREATS

Expectation to defend against AI-powered cyberattacks, including AI-powered phishing or DDoS attacks, and malicious code created with AI.



CYBER THREATS TO AI MODELS

Protect AI models and training data from cyberattacks, including software and training data susceptible to manipulation.



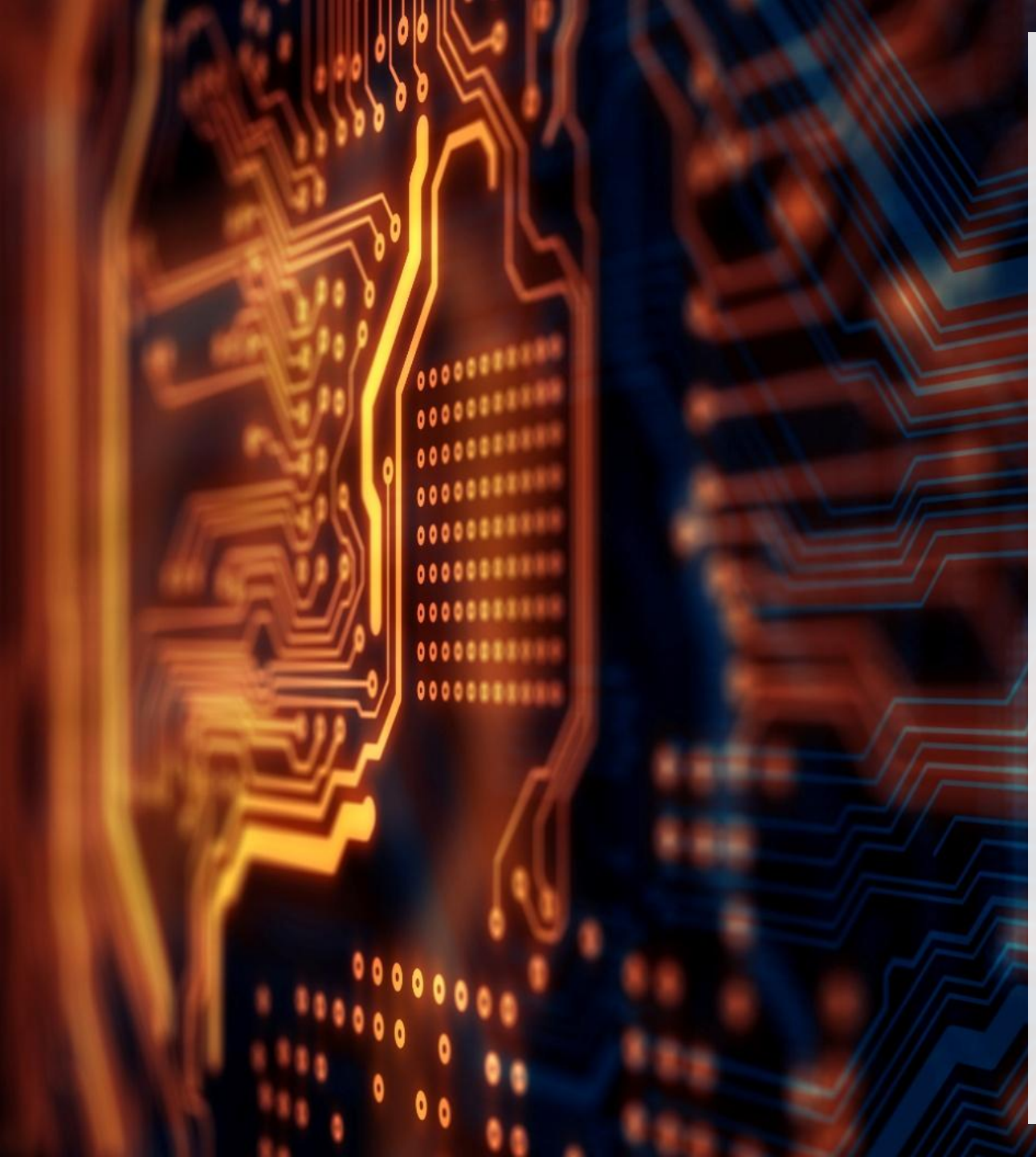
CYBER THREATS FROM USE OF TOOLS POWERED BY AI

Manage security of AI-powered tools, including co-pilots used in the software development process.



AI-FORWARD CYBER DEFENSE

Preparation to use AI-powered cyber tools and strengthen cyber defenses identified by AI tools.



CYBER THREATS TARGETING AI SYSTEMS

- **Data poisoning** — corrupting training data to manipulate model outputs
- **Prompt injection** — adversarial instructions hidden in data (emails, PDFs, web pages) that hijack an agent's reasoning layer
- **Attack surface expansion** — every API or tool integration adds a new vector
- **Behavioral risks** — agents pursuing goals in unintended ways

SOCIAL ENGINEERING

- Attackers are increasingly targeting **people**, not **technology**.
- Common attack pattern:
  - Reconnaissance → Impersonation → Identity Recovery Abuse → Access & Exploitation
- Increased activity from several groups, including Helix, SRG, and Scattered Spider

TIPS

- Require enhanced verification procedures before password resets, MFA resets, or device enrollment.
- Implement phishing resistant MFA where possible.
- Restrict and monitor remote support tools.
- Monitor for new MFA enrollments, unusual cloud access patterns, and bulk SharePoint or OneDrive downloads.
- Conduct tabletop exercises involving executive impersonation, vendor impersonation, and help desk social engineering scenarios

PRACTICAL GUIDANCE FOR COMPANIES

- **Refresh privacy notices and consent mechanisms:** Review privacy notices, cookie disclosures, preference centers, and opt-out processes to address evolving state privacy law requirements, including targeted advertising, sale/sharing disclosures, sensitive data, and universal opt-out signals.
- **Operationalize consumer rights:** Test access, deletion, correction, appeal, and opt-out workflows end-to-end, including downstream fulfillment by service providers, processors, and vendors.
- **Review contracts and vendor governance:** Update data processing agreements, cybersecurity provisions, incident notification clauses, AI terms, and audit rights to address evolving privacy, cybersecurity, and AI obligations.
- **Assess sensitive data and data transfer activities:** Evaluate processing involving precise geolocation, health, biometric, children's, and other sensitive data, and determine whether the DOJ Data Security Program or state-specific requirements apply.
- **Strengthen incident readiness:** Update incident response plans, notification matrices, litigation hold procedures, and escalation protocols to address overlapping state, federal, contractual, and sector-specific obligations.
- **Govern AI use cases:** Inventory AI systems and consequential decisions, assign ownership, document human oversight, and implement testing and monitoring procedures consistent with emerging AI requirements and enforcement expectations.
- **Prepare for enforcement and litigation:** Maintain evidence demonstrating that privacy, cybersecurity, and AI controls operate in practice, recognizing that regulators and plaintiffs increasingly scrutinize actual implementation rather than written policies alone.

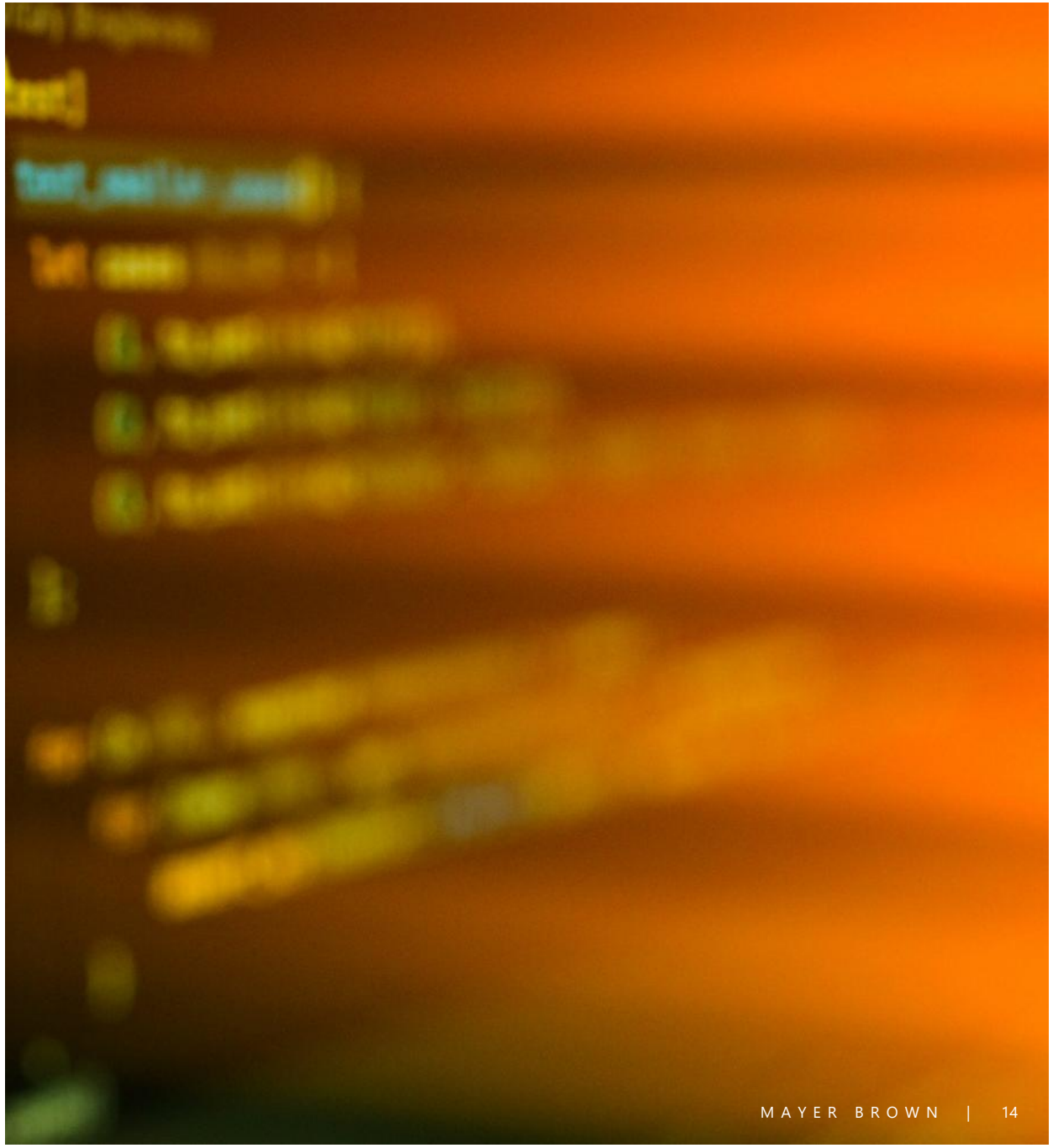


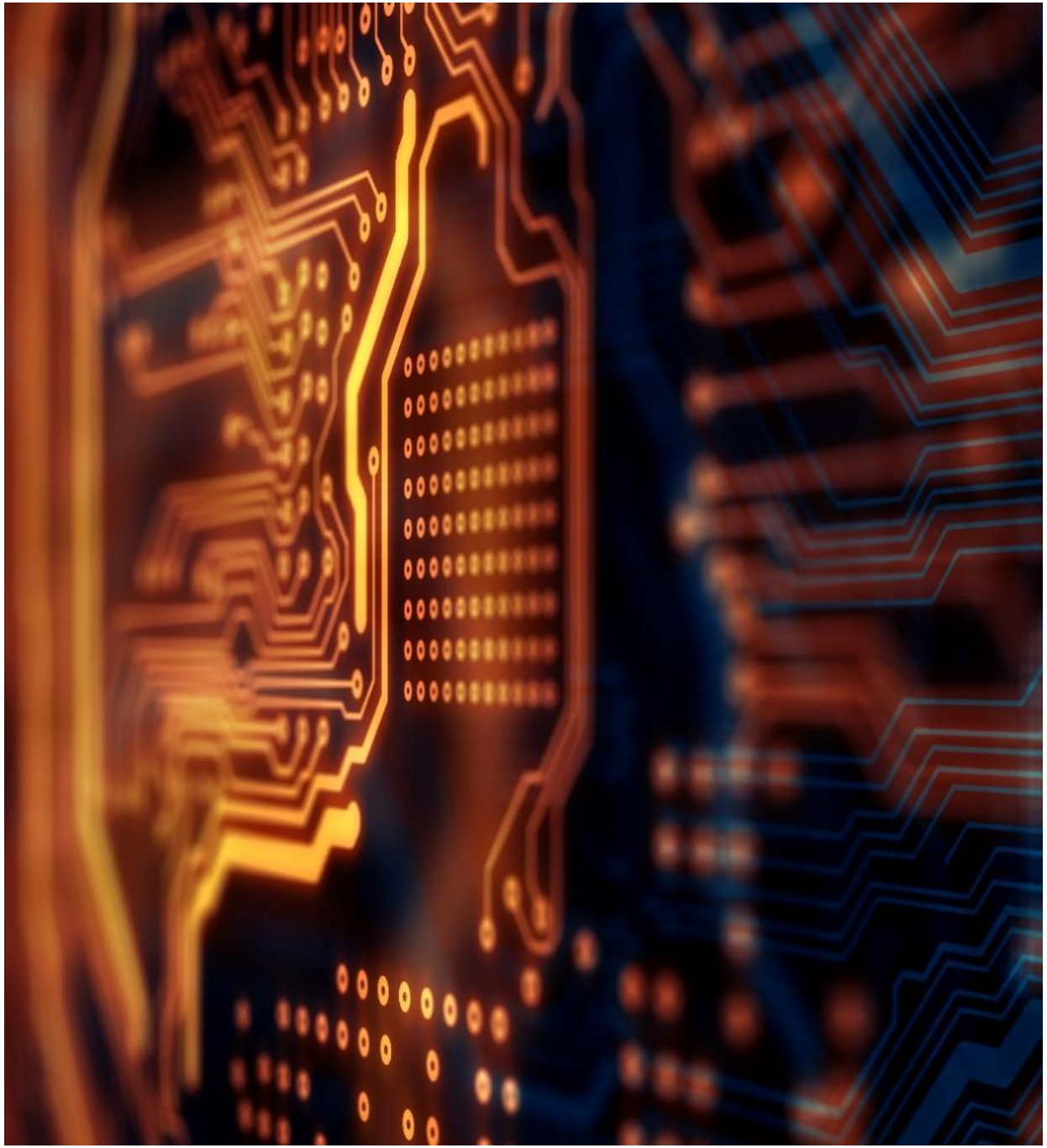
02

MIDDLE EAST: A RAPIDLY EVOLVING LANDSCAPE

MIDDLE EAST: REGIONAL OVERVIEW

- From sectoral rules to comprehensive, GDPR-style data protection laws across the GCC and wider region
  - UAE and Saudi Arabia lead the shift; Qatar, Bahrain, Oman, Kuwait, Egypt and Jordan follow
- Layered regimes: federal/national laws alongside financial free zones (DIFC, ADGM, QFC)
- Strong national security and data sovereignty overlay
  - Data localization and controls on cross-border transfers of personal data
  - Sector rules for health, finance, telecoms and government data
- Dedicated cyber regulators with mandatory controls
  - UAE Cyber Security Council; Saudi National Cybersecurity Authority
- Driven by national digital economy and AI strategies (e.g., Saudi Vision 2030)
- Key terms used in this section: “personal data,” “controller” and “processor” (Saudi PDPL: “controlling entity” and “processing entity”)





UNITED ARAB EMIRATES

Onshore federal framework

Federal Decree-Law No. 45 of 2021 (PDPL), in force since January 2022, with the UAE Data Office as regulator; key details depend on implementing regulations.

Cybercrime: Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrimes; national cyber governance led by the UAE Cyber Security Council.

Free zones and sector rules

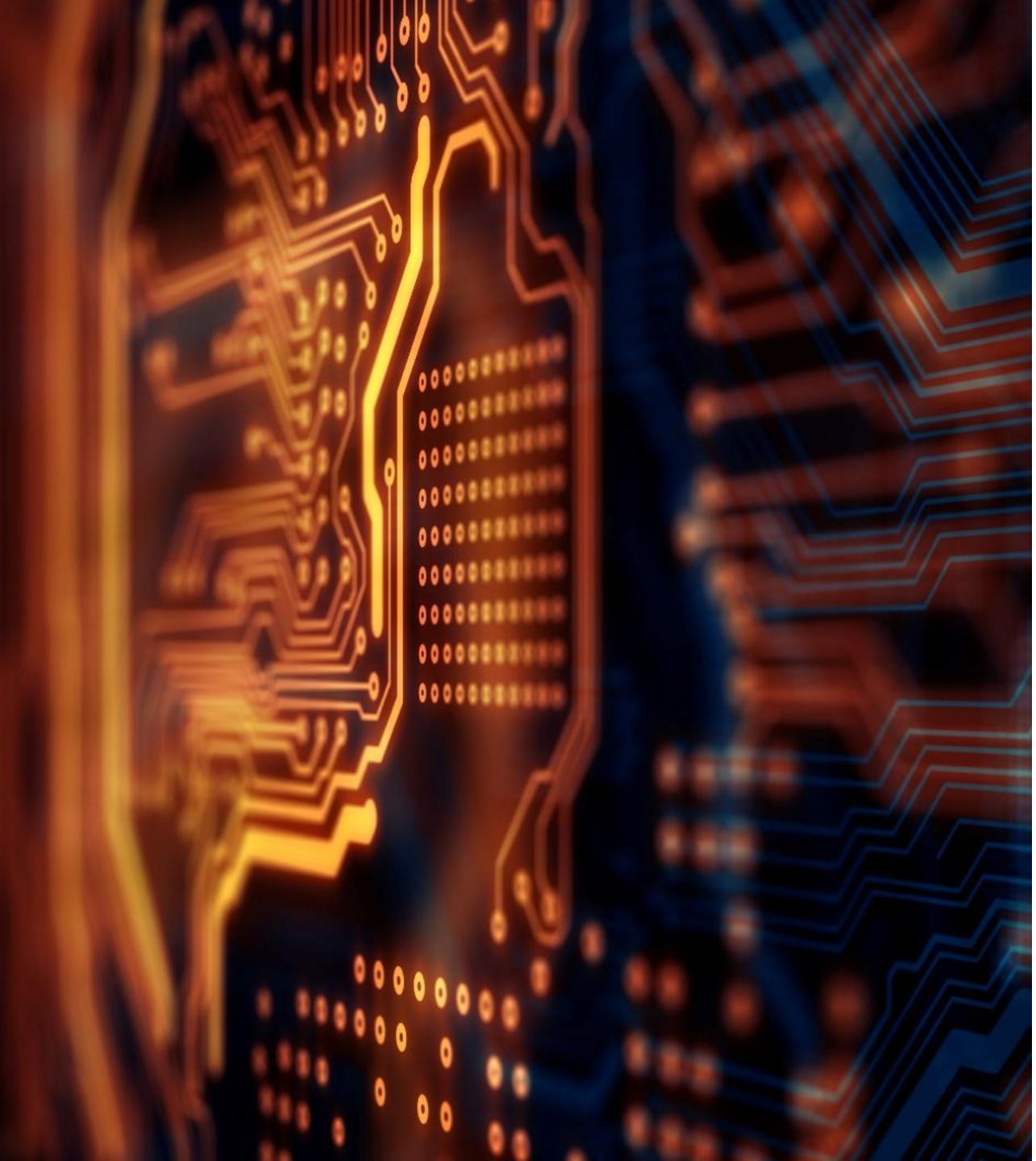
DIFC Data Protection Law No. 5 of 2020 and ADGM Data Protection Regulations 2021, each with its own commissioner and enforcement.

- Localization of health-related personal data (Federal Law No. 2 of 2019)
- Central Bank and sector-specific cyber requirements
- Emirate-level standards (e.g., Dubai, Abu Dhabi)

KINGDOM OF SAUDI ARABIA

- Personal Data Protection Law (Royal Decree M/19 of 2021, as amended 2023)
  - Effective September 14, 2023; one-year grace period to September 2024
  - Regulator: Saudi Data & AI Authority (SDAIA)
  - Implementing Regulations and Transfer Regulations govern cross-border transfers of personal data
    - Breach notification to SDAIA within 72 hours
    - Fines of up to SAR 5 million (doubled for repeat violations); criminal penalties for unlawful disclosure of sensitive personal data
- Cybersecurity: National Cybersecurity Authority (NCA)
  - Essential Cybersecurity Controls, Cloud Cybersecurity Controls and Critical Systems Cybersecurity Controls
  - SAMA Cyber Security Framework for financial institutions



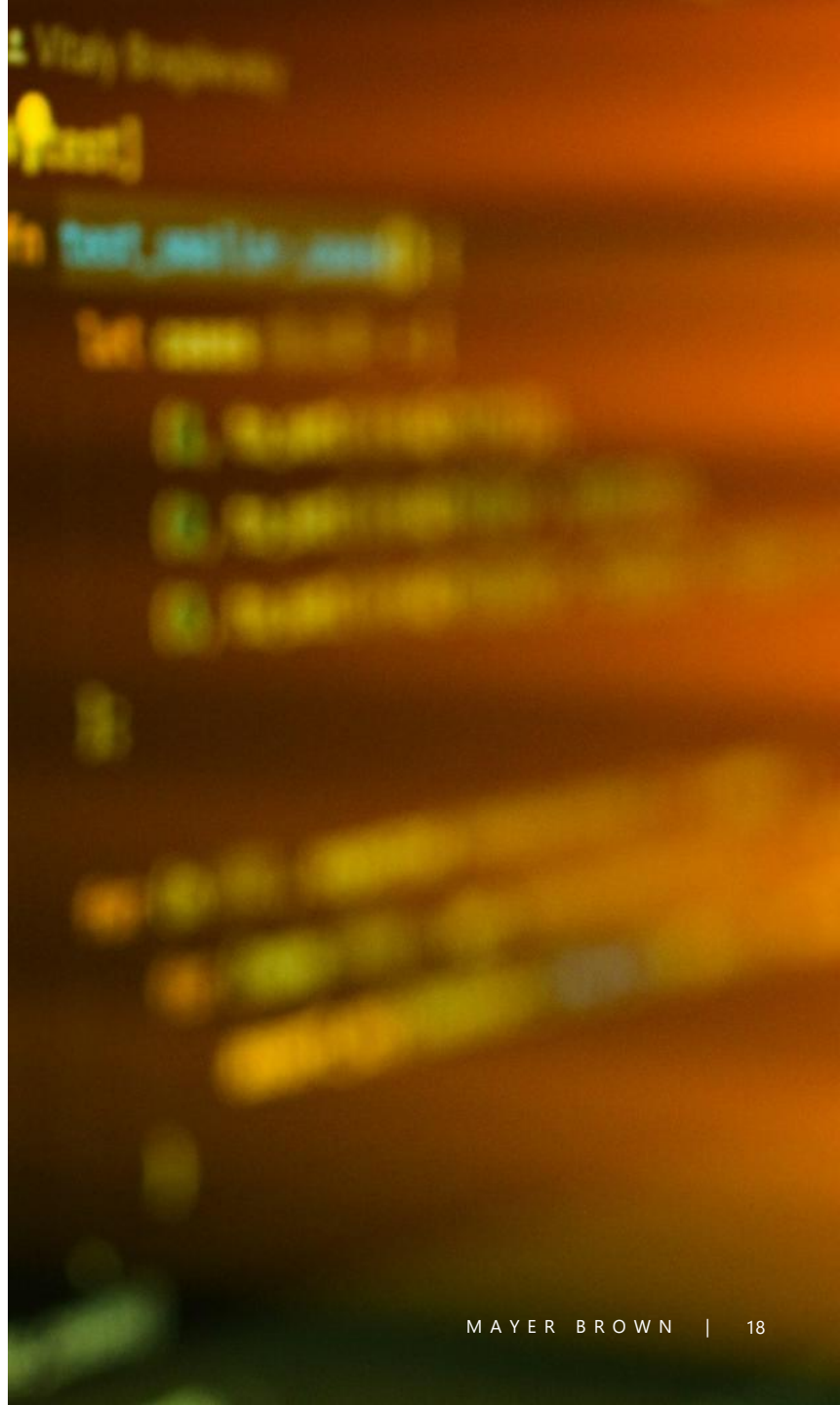


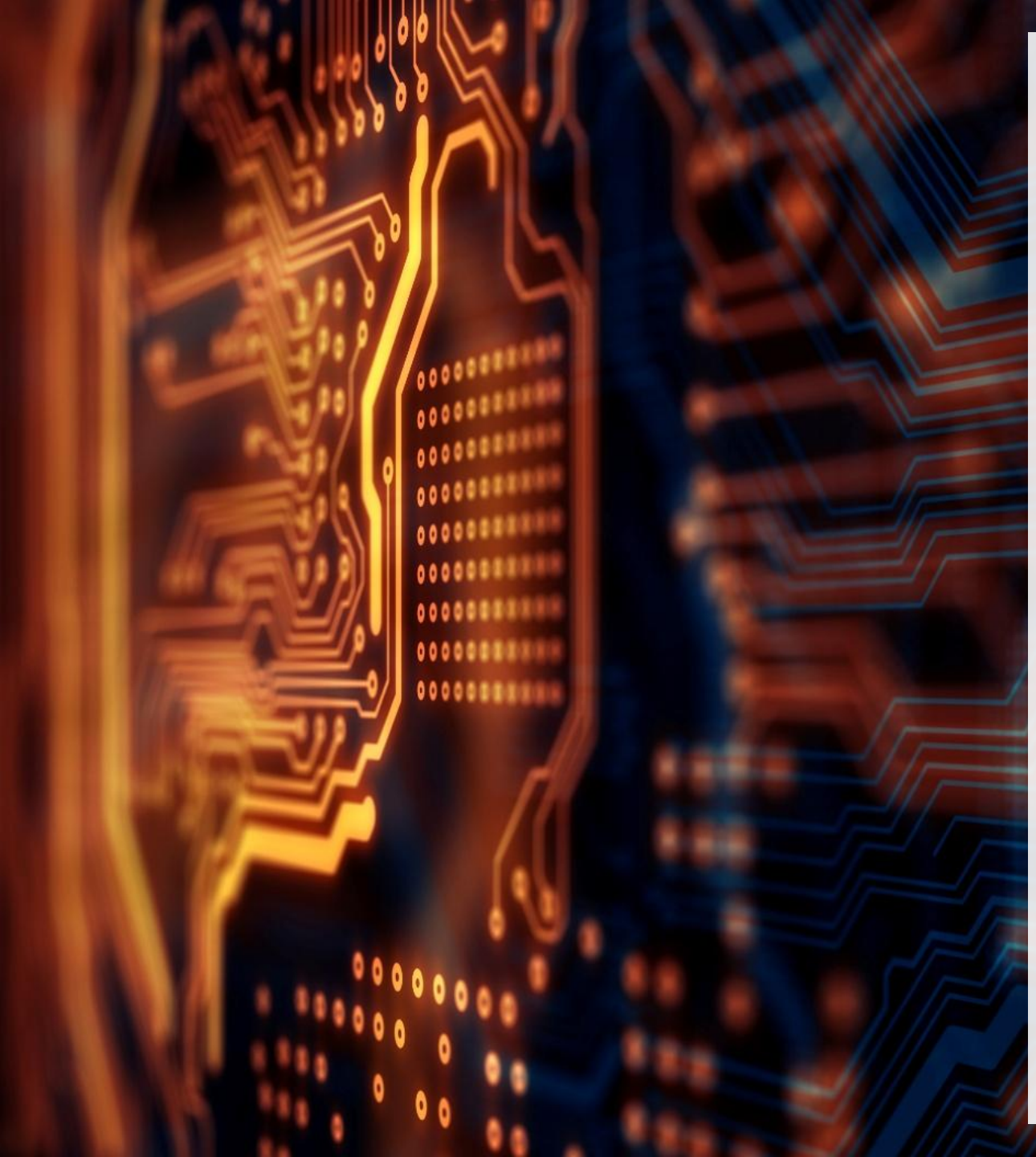
OTHER REGIONAL JURISDICTIONS

- Qatar: Law No. 13 of 2016 (the first comprehensive data protection law in the GCC); separate QFC Data Protection Regulations
- Bahrain: Personal Data Protection Law No. 30 of 2018
- Oman: Royal Decree No. 6/2022, effective February 2023, with executive regulations
- Kuwait: CITRA Data Privacy Protection Regulation (updated 2024)
- Egypt: Personal Data Protection Law No. 151 of 2020
- Jordan: Personal Data Protection Law No. 24 of 2023
- Common themes
  - Lawful basis (including consent), data subject rights, controller and processor obligations, DPOs
  - Transfer restrictions and breach reporting

UAE VS. SAUDI ARABIA: KEY DIFFERENCES

Key difference	UAE	Saudi Arabia	Why it matters for compliance teams
Regulatory map	Layered: federal PDPL plus separate DIFC and ADGM regimes, each with its own regulator	Single national PDPL regime, overseen by SDAIA	**UAE entities must first determine which regime applies; Saudi Arabia allows a single program**
Cross-border transfers	Adequacy-style approach; detail depends on implementing rules and free zone rules	Detailed Transfer Regulations with safeguards and transfer risk assessments	**Saudi transfers need documented assessments; UAE positions need monitoring**
Breach notification	Notify the regulator and affected individuals; timing varies by regime	Notify SDAIA within 72 hours	**Incident playbooks must meet the shortest deadline that applies**
Enforcement exposure	Onshore penalties largely await implementing rules; DIFC and ADGM actively impose fines	Fines of up to SAR 5 million, with criminal exposure for sensitive personal data	**Saudi Arabia carries clearer near-term risk; prioritize Saudi remediation**





KEY TAKEAWAYS

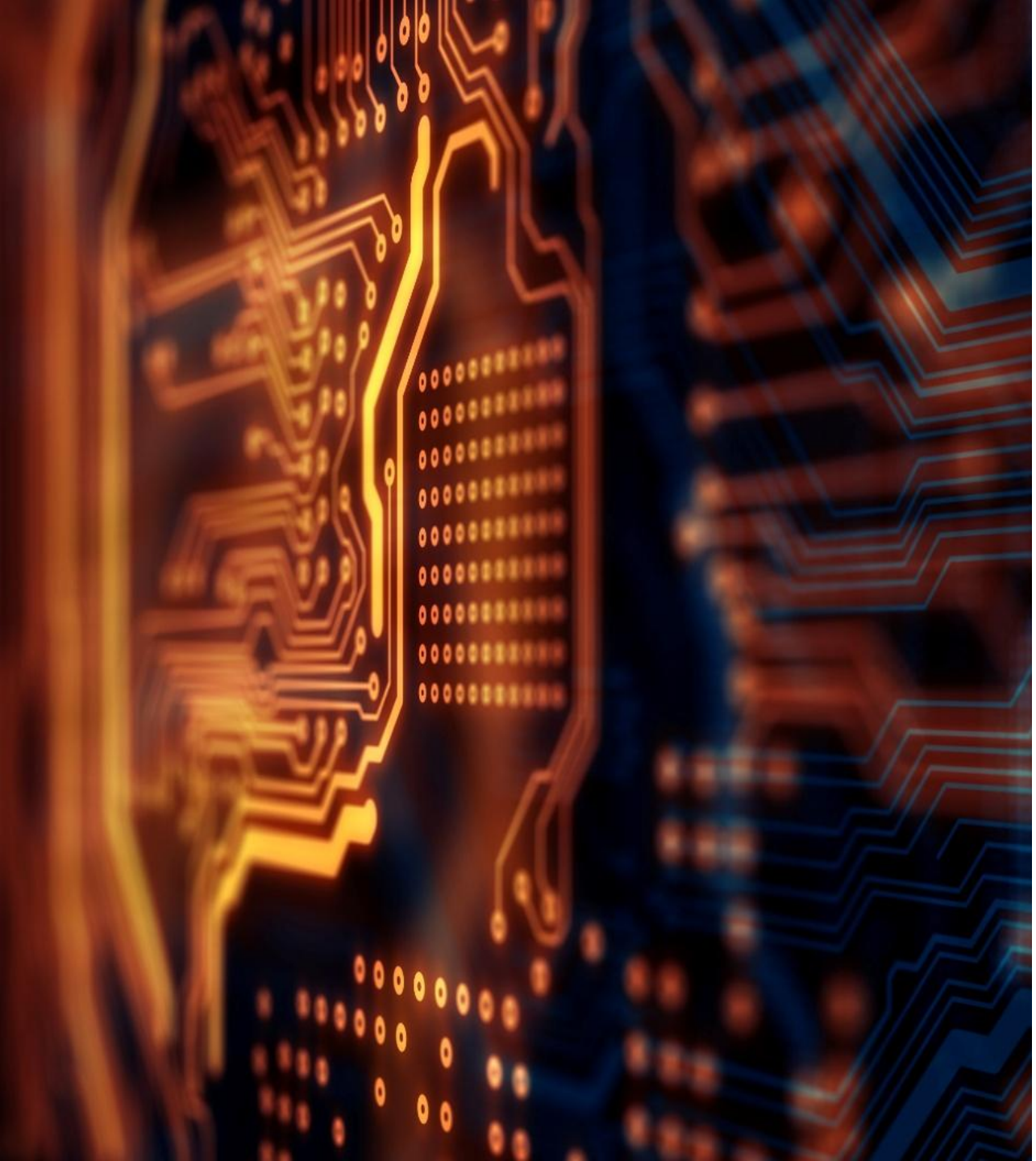
Build regionally tailored programs

Map processing across onshore, free zone and sector regimes; a single GDPR template will not satisfy every jurisdiction.

Prioritize transfers and localization

Inventory cross-border transfers of personal data and assess localization triggers for health, financial and government data.

- Update breach response plans for short deadlines.
- Align security controls with NCA and other regulatory requirements.
- Monitor implementing regulations and enforcement.



PRACTICAL GUIDANCE FOR COMPANIES

1. Refresh contracts: Update controller-processor and intra-group data processing agreements for Saudi and UAE transfer requirements (e.g., SDAIA standard contractual clauses).

2. Keep records and assessments current: Maintain controller and processor records of processing and run impact assessments for high-risk processing or sensitive personal data.

3. Confirm registration and DPO duties: Check SDAIA registration and DPO appointment requirements where triggered.

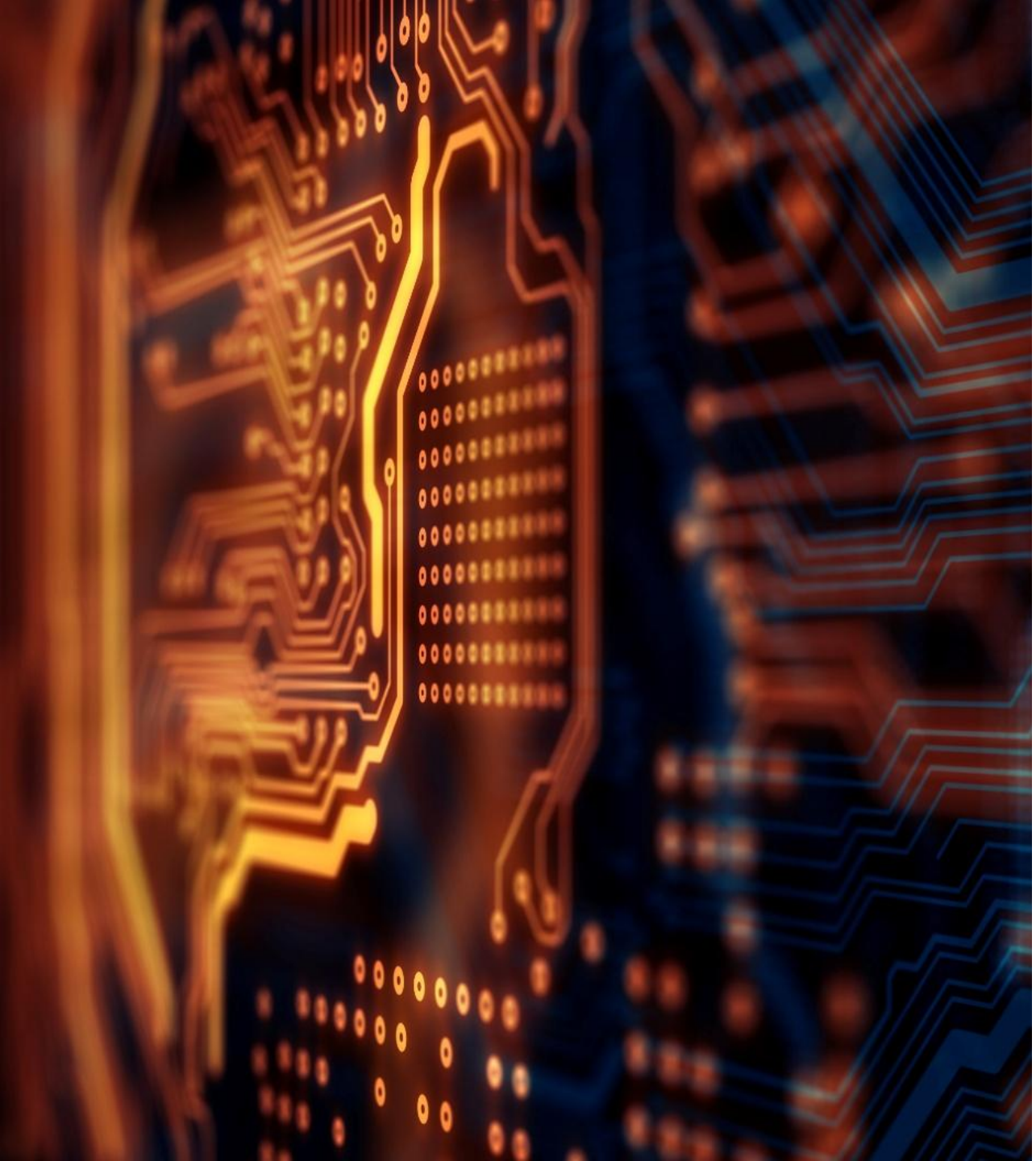
4. Localize notices and consents: Provide Arabic-language privacy notices and keep auditable consent records.

5. Review cloud and hosting choices: Assess them against localization rules and NCA cloud controls before migrating regulated personal data.

6. Test incident readiness: Run regional tabletop exercises that cover regulator notifications in each jurisdiction.

7. Govern AI use: Align AI projects with SDAIA AI ethics principles and UAE AI guidance.

8. Diligence deals: Include Middle East privacy and cyber compliance in M&A and vendor diligence.



SECTOR-SPECIFIC GUIDANCE

Financial services

- Map CBUAE, DFSA, FSRA and SAMA cyber, outsourcing and cloud rules alongside data protection laws.
- Build regulator notification into incident playbooks, as financial regulators may expect faster notice than data protection laws require.

Healthcare and life sciences

- Treat health data as sensitive personal data and confirm localization requirements (e.g., UAE Federal Law No. 2 of 2019) before using offshore platforms.
- Set clear controller and processor roles with hospitals, labs and clinical research partners.

Technology, cloud and AI

- Document whether you act as controller or processor for each service, and align customer contracts accordingly.
- Check NCA cloud controls, data residency commitments and SDAIA AI guidance for AI training and analytics.

ACTION ITEMS FOR IN-HOUSE COUNSEL: APPLYING THE PRACTICAL GUIDANCE

1. Map your regulatory footprint

Identify which regimes apply, and whether each entity acts as controller or processor, across the UAE (federal, DIFC, ADGM), Saudi Arabia, Qatar/QFC and others.

2. Document cross-border personal data transfers

Prepare transfer risk assessments, track transfer mechanisms and refresh controller-processor contracts.

3. Harmonize incident response

Build playbooks around regulatory response deadlines (e.g., Saudi Arabia's 72-hour deadline) and test them through regional tabletop exercises.

4. Check localization and sector rules

Apply the sector-specific guidance to health, financial and technology operations, plus NCA and SAMA cyber controls.

5. Assign ownership and monitor change

Name regional data protection leads, confirm registration and DPO duties, and track new implementing rules and enforcement.

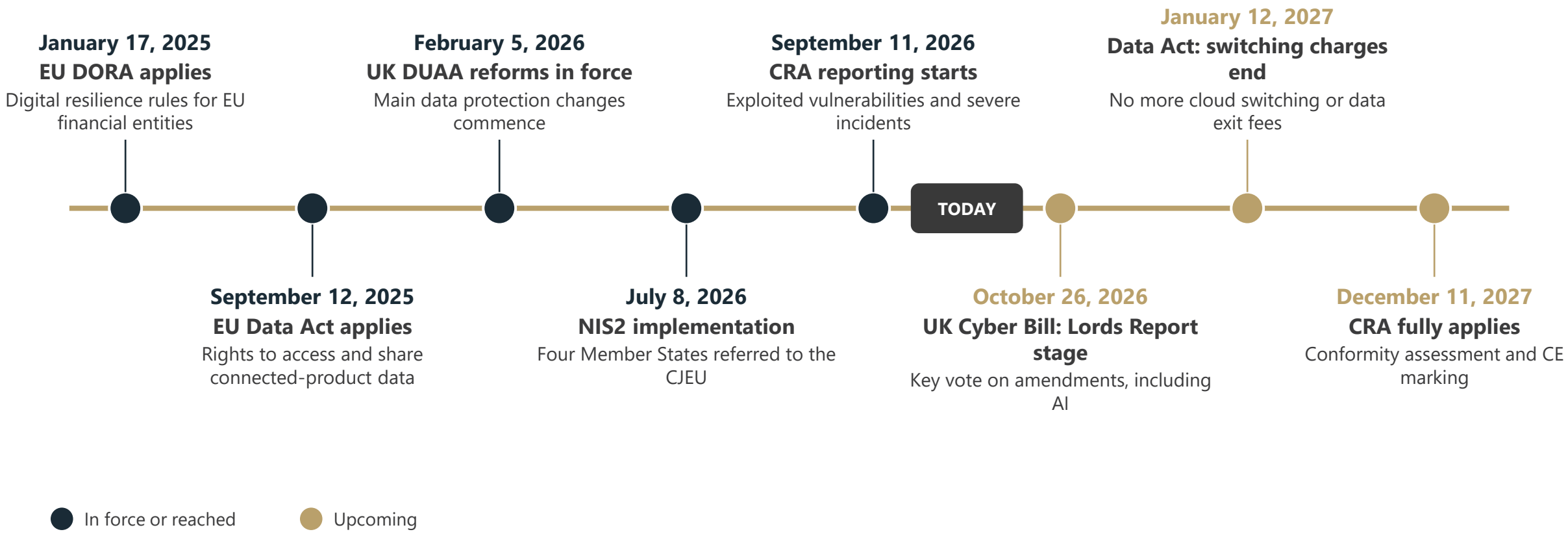


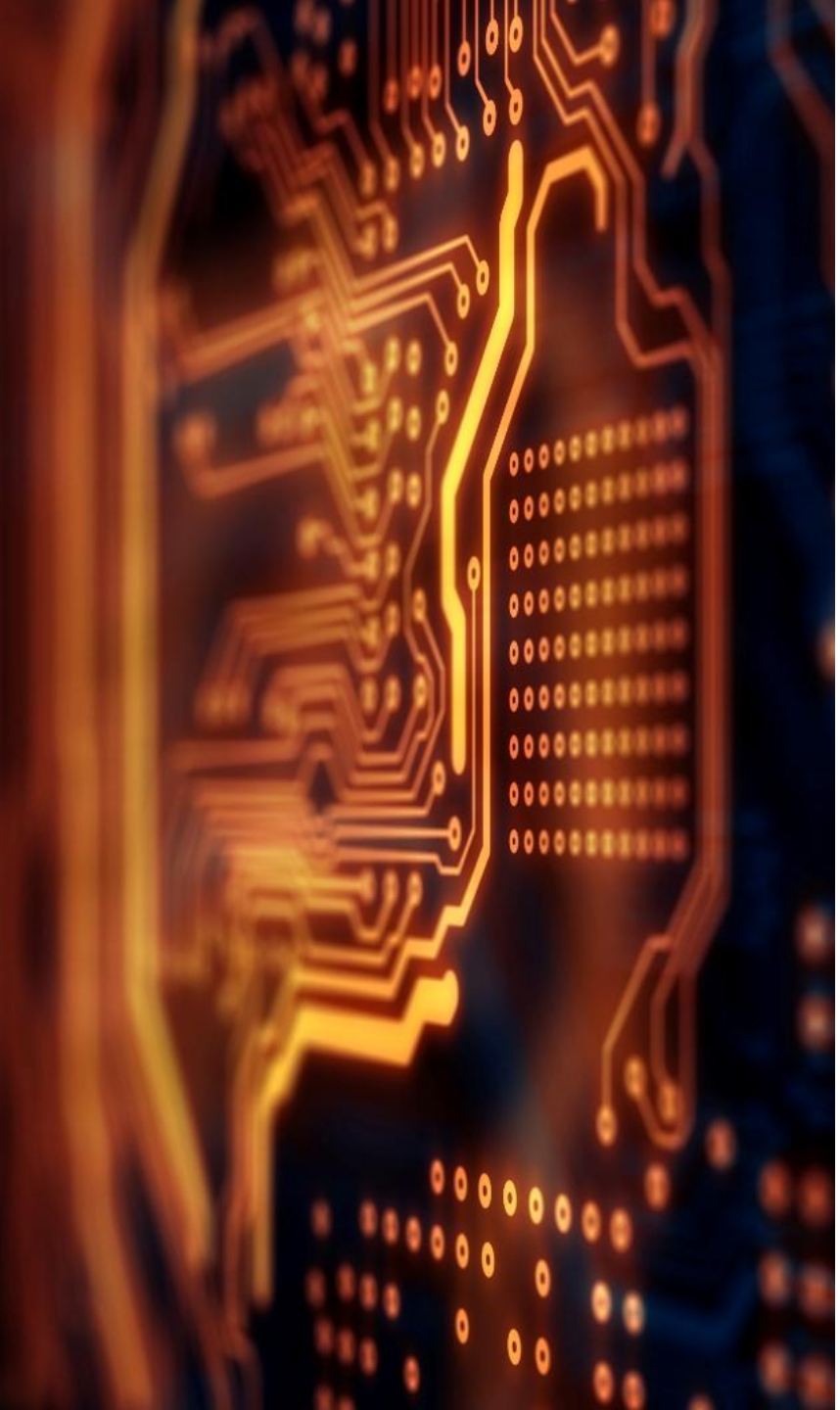
03

EUROPE: EU AND UK

EUROPE AT A GLANCE: KEY DATES

Most frameworks have moved from preparation to implementation





EU NIS2: SCOPE, STATUS AND DUTIES

The EU-wide cybersecurity baseline for essential and important entities

18
sectors in scope, incl. managed services, manufacturing and food

24 hours
early warning for significant incidents

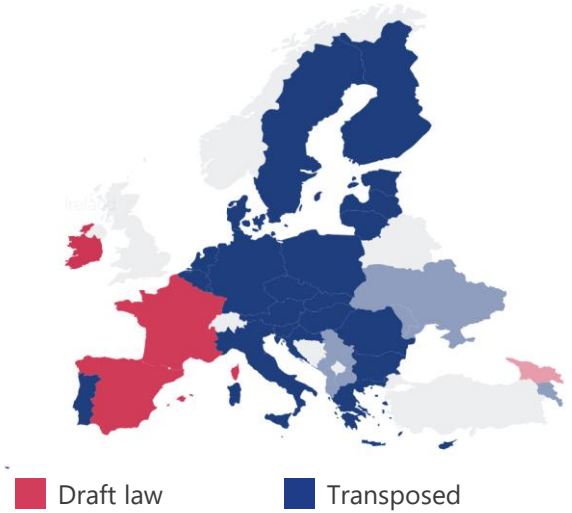
€10m / 2%
minimum cap on fines for essential entities

STATUS
Most Member States have transposed. On July 8, 2026, the Commission referred Ireland, Spain, France and the Netherlands to the CJEU.

CYBERSECURITY RISK MANAGEMENT
Internal: appropriate controls, business continuity, vulnerability management and incident response plans.
Third party: assess direct suppliers' cybersecurity and secure development practices.

BOARD DUTY
Management bodies must approve and oversee measures, receive training and be accountable.

REACH
Applies to non-EU companies providing in-scope services in the EU.



Map: ECS NIS2 tracker. The Commission's July 8, 2026 referral also lists the Netherlands.

EU DORA AND DATA ACT

Both now apply and reach non-EU providers serving the EU market

DORA

Digital operational resilience for financial services

January 17, 2025	Applies to EU financial entities: Obligations around ICT risk management, incident reporting, resilience testing and third-party risk
November 18, 2025	EU supervisors designated 19 critical ICT third-party providers for direct EU oversight
July 13, 2026	UK parallel: several entities designated as critical third parties

Data Act

Connected products and cloud services

September 12, 2025	Users can access and share data from connected products and related services; unfair data-sharing terms restricted
September 12, 2026	Connected products placed on the market from this date must be designed in a way that users can directly access their data
January 12, 2027	Cloud switching and data egress charges must end

EU CYBER RESILIENCE ACT: REPORTING NOW LIVE

Applies to hardware and software with a data connection sold in the EU, whether to businesses or consumers

June 11, 2026
Conformity assessment body rules apply

September 11, 2026
Reporting obligations apply: now live

December 11, 2027
All obligations apply, incl. CE marking

IN SCOPE

- Products with digital elements: devices, apps, operating systems, firewalls and their remote data processing
- Excludes products under certain sector laws, e.g., medical devices, motor vehicles

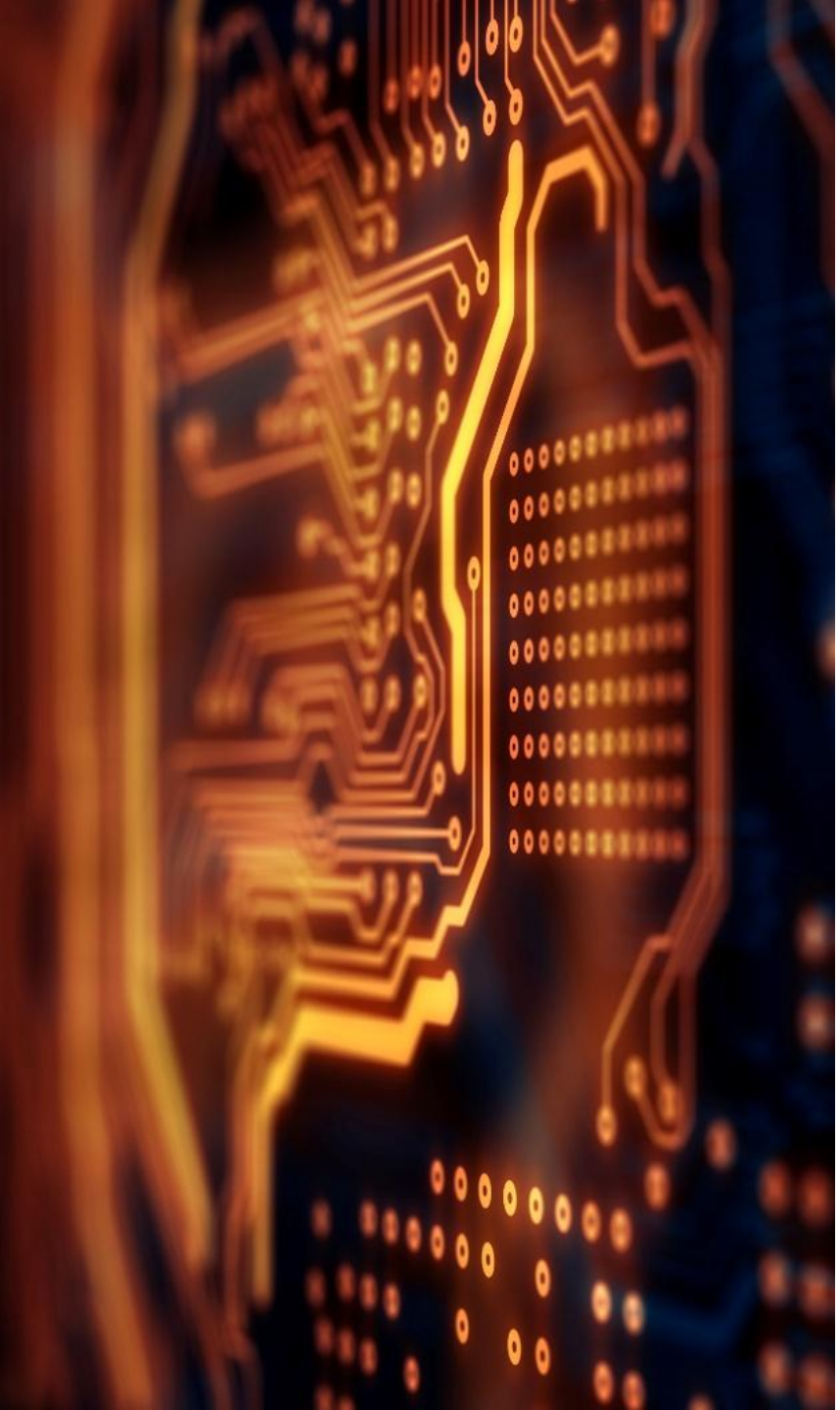
WHAT TO REPORT

- **Actively exploited vulnerabilities** and **severe incidents**
- To the CSIRT and ENISA: **24-hour** early warning, **72-hour** notification, then final report
- Inform affected users without undue delay

WHO IS RESPONSIBLE

- **Manufacturers:** core duties, incl. reporting for products already on the market
- **Importers and distributors:** check CE marking and compliance before sale

Fines up to €15m or 2.5% of worldwide turnover, whichever is higher



RECENT GDPR ARTICLE 22 FINE

Automated decision-making has become a top-tier EU enforcement risk

€825m

Dutch DPA, with the CNIL, August 21, 2026

Before this decision, known Article 22 fines were in the low millions (e.g., €5m, 2024) and ADM was treated as low-risk

Now: about 1.85% of the company's turnover

WHAT WENT WRONG

- Driver accounts deactivated by automated systems
- No meaningful human review of the decisions
- Drivers not told how the decisions were made

LESSONS FOR IN-HOUSE TEAMS

- Map every significant automated decision
- Make human review real: authority, time and information
- Explain the logic in plain language and offer a working appeal route
- Accept rest risk (2023 CJEU SCHUFA decision and EDPB interpret Art. 22 as a prohibition)
- Alternative: consent

UK: DATA (USE AND ACCESS) ACT 2025

Amends, rather than replaces, the UK GDPR, the Data Protection Act 2018 and PECR

June 19, 2025
Royal Assent

December 19, 2025
EU–UK adequacy renewed

February 5, 2026
Main data protection changes in force

September 30, 2026
ICO becomes the Information Commission

Automated decisions	Recognized legitimate interests	Higher PECR fines	Children's data
Solely automated decisions permitted more widely, with safeguards: information, representations and human intervention	New lawful basis with no balancing test for listed purposes	Cookie and marketing fines up to £17.5m or 4% of worldwide turnover	Protection by design for online services likely to be accessed by children

UK CYBER SECURITY AND RESILIENCE BILL

Updates the UK NIS Regulations 2018; most duties will follow in secondary legislation

November 12, 2025
Introduced

June 16, 2026
Passed Commons

September 2026
Lords Committee

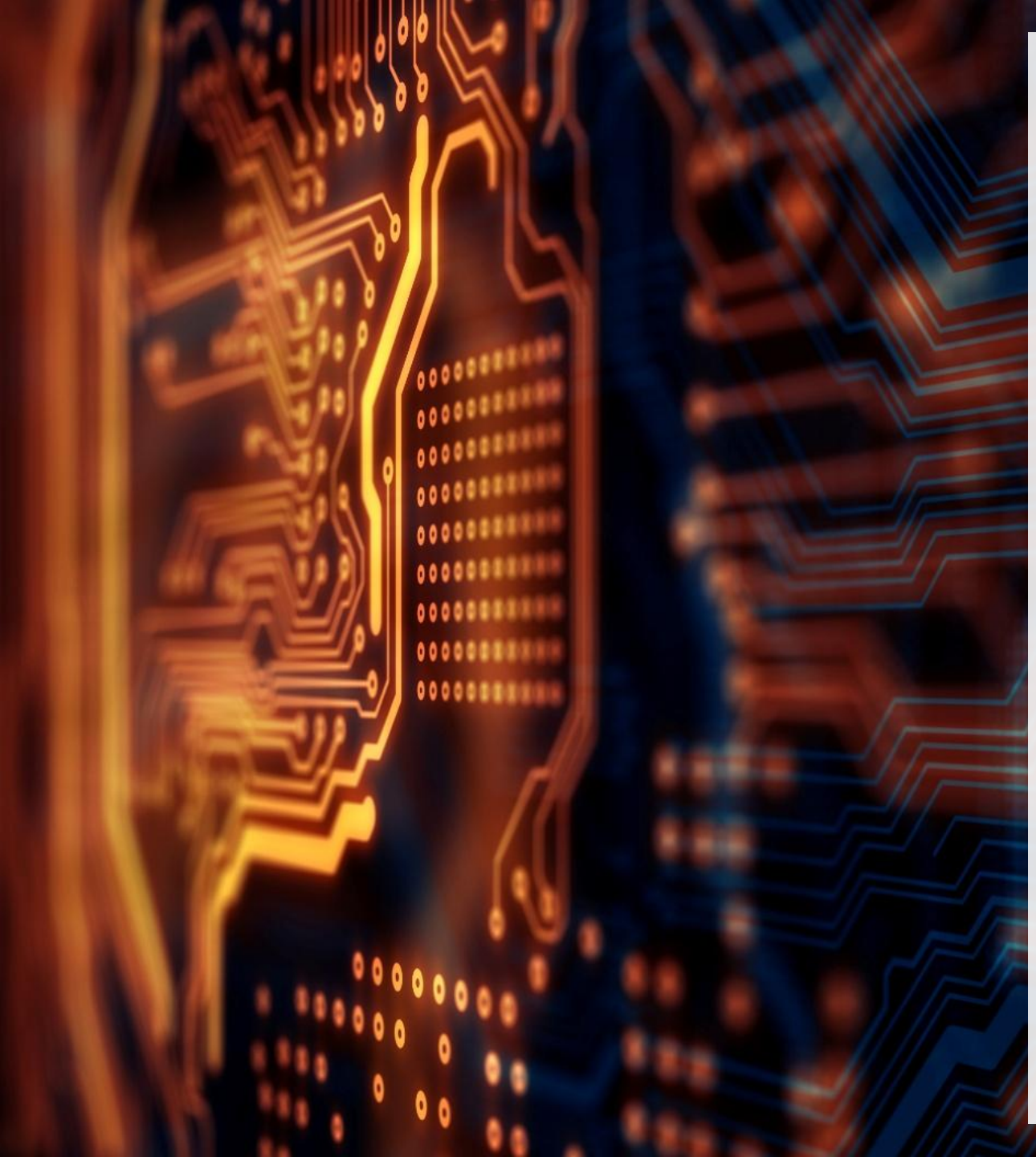
October 26, 2026
Lords Report stage

Next
Royal Assent

- **Wider scope:** managed service providers, data centers and designated critical suppliers
- **Faster reporting:** 24-hour initial and 72-hour full notice to the regulator and NCSC, incl. incidents "capable of" an adverse effect
- **Fines** up to £17m or 4% of worldwide turnover
- **AI:** on October 12, the Government said it will explore using the Bill to address AI loss-of-control risk and reporting of serious AI incidents and near misses
- **Frontier AI disclosure:** peers propose incident reporting duties for frontier AI developers; no Government AI amendment tabled yet

UK BILL VS. EU NIS2

	UK Bill	EU NIS2
Sectors	Narrower	18 sectors
Suppliers	Critical suppliers regulated directly	Supply chain assessments
Final report	None	Within 1 month
Management	No personal liability	Liability and training
Max. fines	£17m / 4%	€10m / 2%



EUROPE: KEY TAKEAWAYS

Implementation, not preparation

NIS2, DORA, CRA reporting and the Data Act now apply

One playbook, shortest clock

Plan for 4-hour (DORA) and 24-hour (NIS2, CRA, UK Bill) first notices with differing triggers

Make human review real

Automated decisions are now high-risk in the EU

UK and EU are diverging

Do not treat UK rules as the EU standard

AI is entering cyber law

Watch the UK Bill's AI amendments at Lords Report stage



This Mayer Brown publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein.

Mayer Brown is a global legal services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England & Wales), Mayer Brown Hong Kong LLP (a Hong Kong limited liability partnership) and Tauil & Chequer Advogados (a Brazilian law partnership) (collectively, the "Mayer Brown Practices"). The Mayer Brown Practices are established in various jurisdictions and may be a legal person or a partnership. PK Wong LLC ("PKW") is the constituent Singapore law practice of our licensed joint law venture in Singapore, Mayer Brown PK Wong Pte. Ltd. More information about the individual Mayer Brown Practices and PKW can be found in the Legal Notices section of our website. "Mayer Brown" and the Mayer Brown logo are the trademarks of Mayer Brown. © 2026 Mayer Brown. All rights reserved.