REGULATORY MEMORANDUM

# Digital Sovereignty & Critical Regulatory Frameworks

*For Chief Information Officers*

**PREPARED BY** Steven De Schrijver, Partner, Allegiance Law
**OCCASION** CIONET: The Sovereignty Play, 23 June 2026
**CLASSIFICATION** Strictly Confidential: For CIONET CIO Community
**SCOPE** 16 regulatory framework across the US, the EU, the UK, and Australia

ALLEGIANCE LAW

## Purpose of this Memorandum

This memorandum provides CIOs with a concise reference guide to the principal regulatory frameworks governing data access, cloud sovereignty, cybersecurity, and operational resilience across four key jurisdictions. For each framework, we set out what the regulation is, what it requires of companies, who it applies to, and why it matters for your organisation's digital sovereignty strategy. This document should be read alongside the practical control questions raised during the CIONET session: the legal landscape described here is the framework within which your technical and contractual architecture must operate.

# EUROPEAN UNION — REGULATORY FRAMEWORKS

## 1. General Data Protection Regulation (GDPR)

*Jurisdiction: EUROPEAN UNION | Year: 2018*

| | |
|---|---|
| **What is it?** | The GDPR is the EU's foundational data protection regulation, governing the processing of personal data of individuals in the European Economic Area. It establishes principles of lawfulness, purpose limitation, data minimisation, accuracy, storage limitation, and integrity. It regulates all forms of data processing, including storage, transfer, and access, and imposes strict requirements on cross-border data transfers. |
| **Obligations for companies** | Organisations must have a lawful basis for processing personal data, implement appropriate technical and organisational security measures, maintain records of processing activities, conduct data protection impact assessments for high-risk processing, appoint a Data Protection Officer where required, and comply with data subject rights. Transfers to third countries require adequacy decisions, standard contractual clauses, or other approved mechanisms. |
| **Applicable to** | Any organisation established in the EU/EEA, or any organisation outside the EU that processes personal data of EU residents in connection with offering goods/services or monitoring their behaviour. Applies to both controllers and processors. |
| **CIO relevance: Digital Sovereignty** | GDPR is the baseline compliance obligation for virtually every CIO in Belgium. From a sovereignty standpoint, it requires knowing where personal data goes, who processes it, and under what legal regime. The regulation's transfer restrictions are the legal hook that makes US access laws (CLOUD Act, FISA §702) practically relevant: sending personal data to a US provider may be a GDPR violation if that provider cannot guarantee EU-equivalent protection against extraterritorial access. CIOs must map data flows, audit subprocessor chains, and ensure contracts reflect technical reality. |

## 2. Schrems II (Data Protection Commissioner v. Facebook Ireland, C-311/18)

*Jurisdiction: EUROPEAN UNION | Year: 2020*

| | |
|---|---|
| **What is it?** | Schrems II is a landmark ruling of the Court of Justice of the European Union that invalidated the EU-US Privacy Shield as a lawful data transfer mechanism. The Court found that US surveillance law (particularly FISA §702 and Executive Order 12333) does not provide data subjects with an adequate level of protection or effective legal remedies equivalent to those guaranteed in the EU. Standard Contractual Clauses remain valid but require a Transfer Impact Assessment. |
| **Obligations for companies** | Organisations transferring personal data to the US (or any third country) must conduct a Transfer Impact Assessment (TIA) to evaluate whether the destination country's law undermines the contractual protections. Where significant risks are identified, supplementary technical measures (typically encryption with keys controlled outside the US) are required, or the transfer must be suspended. |
| **Applicable to** | All EU/EEA data controllers and processors that transfer personal data to third countries, particularly the United States. The EU-US Data Privacy Framework (2023) provides a current transfer basis, but legal challenges are pending before the CJEU. |
| **CIO relevance: Digital Sovereignty** | Schrems II brought the tension between GDPR and US surveillance law into sharp legal focus. For CIOs, it means that contractual assurances from US cloud providers are insufficient on their own: the TIA process requires a genuine technical assessment of access risks. Customer-held encryption keys are the most robust supplementary measure available. CIOs should treat the current EU-US Data Privacy Framework as legally uncertain pending further CJEU proceedings. |

## 3. NIS 2 Directive (Directive on Security of Network and Information Systems)

*Jurisdiction: EUROPEAN UNION | Year: 2022 / transposed in Belgium: October 2024*

| | |
|---|---|
| **What is it?** | NIS 2 significantly expands the scope of the original NIS Directive (2016). It establishes cybersecurity obligations for a much broader set of sectors (including energy, transport, health, digital infrastructure, cloud services, managed service providers, and public administration) covering both 'essential' and 'important' entities. It introduces supply chain security requirements and mandates 24-hour incident reporting. |
| **Obligations for companies** | In-scope entities must implement risk management measures (access control, encryption, vulnerability management, business continuity), conduct security assessments of their supply chain, and report significant incidents to the national authority (CCB in Belgium) within 24 hours (early warning) and 72 hours (full notification). Senior management is personally accountable for compliance. Fines can reach €10M or 2% of global turnover for essential entities. |
| **Applicable to** | Medium and large enterprises in a broad range of sectors, including cloud computing services, digital infrastructure, and managed service providers. Small entities in critical sectors may also be in scope. In Belgium, transposed via the NIS2 Act (October 2024). |
| **CIO relevance: Digital Sovereignty** | NIS 2 fundamentally changes the CIO's vendor management responsibilities. Supply chain risk is now explicitly in scope: you must assess the cybersecurity practices of your cloud and IT service providers, not just sign a contract and move on. The 24-hour reporting obligation requires mature incident detection capabilities. Personal liability for senior management creates boardroom urgency. This is the regulation that most directly converts sovereignty theory into operational security practice. |

## 4. DORA (Digital Operational Resilience Act)

*Jurisdiction: EUROPEAN UNION | Year: 2022 / applicable January 2025*

| | |
|---|---|
| **What is it?** | DORA establishes a comprehensive digital operational resilience framework for the EU financial sector. It harmonises ICT risk management requirements across banks, insurers, investment firms, payment institutions, and critical ICT third-party service providers (CTPPs). DORA introduces mandatory ICT incident reporting, digital operational resilience testing (including threat-led penetration testing), and strict oversight of ICT third-party risk. |



ALLEGIANCE LAW

| | |
|---|---|
| **Obligations for companies** | Financial entities must maintain ICT risk management frameworks, classify and report major ICT-related incidents to competent authorities, conduct annual resilience testing (and TLPT for significant institutions), maintain detailed registers of ICT third-party arrangements, assess concentration risk from cloud providers, and include mandatory contractual provisions in all ICT service agreements, including exit strategies and audit rights. |
| **Applicable to** | EU financial entities (banks, insurance companies, investment firms, crypto-asset service providers, payment institutions) and their critical ICT third-party providers. Competent financial supervisors (in Belgium: the NBB and FSMA) supervise compliance. |
| **CIO relevance: Digital Sovereignty** | DORA has directly restructured cloud and IT sourcing in the financial sector. The mandatory contractual provisions (including demonstrated exit strategies, subcontractor transparency, and audit rights) are now minimum standards, not negotiating positions. CIOs in financial institutions must maintain a complete register of ICT third-party arrangements with concentration risk analysis. The requirement for demonstrable exit plans (not just clauses) is the most operationally demanding element, and exactly the 'tabletop exit exercise' recommended in our CIONET session. |

## 5. ePrivacy Directive (Directive 2002/58/EC, as amended)

*Jurisdiction: EUROPEAN UNION | Year: 2002 / amended 2009*

| | |
|---|---|
| **What is it?** | The ePrivacy Directive (colloquially 'the Cookie Law') complements the GDPR by establishing specific rules for electronic communications and covers confidentiality of communications, use of cookies and tracking technologies, direct marketing by electronic means, and access to information stored on terminal equipment. A proposed ePrivacy Regulation has been under negotiation for several years and has not yet been finalised. |
| **Obligations for companies** | Operators of electronic communications networks and services must ensure confidentiality of communications. Websites and applications must obtain prior consent before placing non-essential cookies or accessing information on users' devices. Unsolicited direct marketing by email is restricted. Traffic and location data must be deleted or anonymised when no longer needed for transmission purposes. |
| **Applicable to** | Providers of electronic communications networks and services (telecoms, internet providers), and any organisation operating websites or digital services targeting EU users that use cookies, tracking pixels, or similar technologies. |
| **CIO relevance: Digital Sovereignty** | While ePrivacy is primarily a marketing and communications compliance matter, it has operational significance for CIOs managing digital platforms, employee monitoring systems, and analytics infrastructure. Consent management platforms must be technically robust. For Belgian organisations, the Data Protection Authority (GBA/APD) has been active in enforcement. The delayed ePrivacy Regulation, when finalised, will harmonise and potentially tighten these rules significantly. |

## 6. EU Data Act (Regulation (EU) 2023/2854)

*Jurisdiction: EUROPEAN UNION | Year: 2023 / applicable September 2025*

| | |
|---|---|
| **What is it?** | The EU Data Act is a horizontal regulation that establishes rules on who may access and use data generated by connected products (IoT devices, industrial machinery, consumer electronics) and related services within the EU. It complements the GDPR (which governs personal data) by addressing non-personal and mixed datasets. The Data Act is one of the most significant pieces of cloud legislation the EU has produced: it directly mandates cloud switching rights, prohibits lock-in practices, and requires genuine interoperability between cloud providers. It gives users of connected products a right to access the data generated by their use of those products and to share that data with third parties. It also introduces public sector emergency access rights to privately held data in cases of exceptional need. |
| **Obligations for companies** | Manufacturers of connected products must design devices so that data generated by users is accessible by default. Data holders must make data available to users and, at their request, to nominated third parties on fair, reasonable, and non-discriminatory terms. Cloud service providers face specific obligations: they must remove all technical, contractual, and commercial barriers to switching (including excessive egress fees, which must be reduced to zero by September 2027), ensure interoperability through the use of open standards and APIs, and provide functional data portability in standardised, machine-readable formats. |



ALLEGIANCE LAW

| | |
|---|---|
| | Contracts containing clauses that create disproportionate switching obstacles are unenforceable. The regulation also prohibits cloud providers from using data received from customers to compete against those customers. |
| **Applicable to** | Manufacturers of connected products placed on the EU market, providers of related digital services, data holders sharing data under the Act, and all cloud service providers (IaaS, PaaS, SaaS) offering services in the EU, regardless of where they are established. The cloud switching provisions apply broadly to any provider from whom a customer may wish to migrate. Small and micro-enterprises benefit from reduced obligations in certain contexts. Public sector bodies may invoke emergency data access rights in defined circumstances. |
| **CIO relevance: Digital Sovereignty** | The Data Act is arguably the most operationally significant piece of EU cloud legislation for CIOs, because it is the first to directly regulate vendor lock-in as a legal wrong. From a sovereignty standpoint, this matters enormously: the ability to switch providers (at reasonable cost, in a workable timeframe, with portable data in usable formats) is the practical definition of digital autonomy. CIOs should use the Data Act as direct leverage in vendor negotiations, demanding contractual alignment with its portability and switching requirements now, ahead of full enforcement. The elimination of egress fees (effective September 2027) removes one of the most significant financial barriers to multi-cloud architecture. For organisations with IoT deployments or industrial connected assets, the data access provisions open new possibilities for sharing operational data with third-party analytics or maintenance providers without requiring renegotiation with the original equipment manufacturer. Practically, CIOs should audit current cloud contracts for clauses that create switching barriers (exclusivity provisions, proprietary format lock-in, disproportionate migration fees) and begin flagging these for renegotiation. The Data Act gives you the legal basis to demand better terms. |

### Practical note: Data Act & the memorandum's other EU frameworks

The Data Act interacts directly with several frameworks already covered in this memorandum. Its cloud switching provisions reinforce the exit strategy obligations under DORA (Section 7) and the portability rights that address the lock-in dynamic discussed under Schrems II (Section 5). CADA (Section 16), once enacted, will build on the Data Act's interoperability requirements by tiering them into a sovereignty assurance certification framework. CIOs should treat these instruments as a coherent architecture rather than isolated compliance obligations: together, they establish the legal foundation for genuine operational autonomy from any single cloud provider.

## 7. Cloud and AI Development Act (CADA)

*Jurisdiction: EUROPEAN UNION | Year: Proposed June 2026 / not yet binding*

| | |
|---|---|
| **What is it?** | The Cloud and AI Development Act (CADA) is a legislative proposal announced by the European Commission in June 2026 that establishes a tiered sovereignty assurance framework for cloud and AI services. It builds on the existing EU cloud regulatory landscape (NIS 2, Data Act, AI Act). It introduces standardised assurance levels for cloud security, data access controls, and AI system integrity, with particular relevance for public procurement and critical infrastructure operators. |
| **Obligations for companies** | Under the proposed framework, cloud and AI service providers will be required to obtain tiered certification (Basic, Advanced, Sovereign) from accredited bodies, demonstrating progressive levels of data access controls, jurisdictional independence, and auditability. Public sector bodies and operators of critical infrastructure are expected to use higher-tier certified services for sensitive workloads. Obligations for private sector organisations are currently less defined but will be shaped by procurement requirements cascading through supply chains. |
| **Applicable to** | Cloud service providers operating in the EU market, AI service providers, public sector bodies, operators of essential services, and private sector organisations contracting with regulated entities. Currently a proposal; formal scope and applicability will be determined through legislative negotiation. |
| **CIO relevance: Digital Sovereignty** | CADA is the legislative signal that the European Commission is moving from voluntary frameworks (EUCS) to binding sovereignty assurance requirements. Even as a proposal, it is already shaping vendor roadmaps and public procurement requirements. CIOs should track the tiered structure: what level of certification will their cloud providers achieve, and will their workloads require a higher tier? Planning for CADA-aligned sourcing now avoids |

| | |
|---|---|
| | disruptive transitions later. It also represents the strongest legal lever yet for demanding contractual and technical sovereignty guarantees from hyperscalers operating in Europe. |

# UNITED STATES — REGULATORY FRAMEWORKS

## 8. CLOUD Act (Clarifying Lawful Overseas Use of Data Act)

*Jurisdiction: UNITED STATES | Year: 2018*

| | |
|---|---|
| **What is it?** | The CLOUD Act (2018) empowers US law enforcement authorities to compel US-based technology companies and cloud service providers to disclose data stored on servers anywhere in the world, regardless of the physical location of that data. It overrides geographic boundaries and allows cross-border data access through executive agreements with foreign governments. Critically, it applies even where data is stored in an EU data centre. |
| **Obligations for companies** | Companies subject to US jurisdiction (including all US-headquartered cloud providers) must comply with lawful orders to produce data, even when stored abroad. They may challenge orders that conflict with foreign law, but the burden is high. There is no general obligation to notify the data subject or the relevant foreign authority. |
| **Applicable to** | Any company incorporated or operating in the United States, or any cloud provider subject to US jurisdiction, regardless of where their servers are located. This includes subsidiaries of US groups and entities contracting with US cloud providers. |
| **CIO relevance: Digital Sovereignty** | This is the single most important US legal instrument for digital sovereignty. Even if your data physically resides in Belgium, a US cloud provider remains legally compellable under the CLOUD Act. 'Data residency' guarantees do not shield you from this access regime. CIOs must understand which of their providers are US-incorporated and evaluate whether sensitive workloads should be migrated to providers not subject to US jurisdiction, or protected through customer-held encryption keys that the provider cannot access. |

## 9. FISA Section 702 (Foreign Intelligence Surveillance Act)

*Jurisdiction: UNITED STATES | Year: 1978 / amended 2008, 2018, 2024*

| | |
|---|---|
| **What is it?** | Section 702 of FISA authorises US intelligence agencies (including the NSA) to conduct surveillance of non-US persons located outside the United States without an individual warrant, by compelling US electronic communications service providers to provide access to targeted communications. The PRISM and Upstream collection programmes have operated under this authority. The programme was reauthorised in 2024. |
| **Obligations for companies** | US-based electronic communications service providers (email, cloud, messaging, VoIP) are legally required to assist intelligence agencies in collecting targeted communications. Providers are prohibited from disclosing that they have received such orders (gag orders apply). Non-US organisations have no direct obligations but bear the risk of surveillance. |
| **Applicable to** | Directly binding on US electronic communications service providers. Indirectly affects all organisations globally that use US-based cloud or communications services, as their data may be subject to collection under this authority. |
| **CIO relevance: Digital Sovereignty** | FISA §702 was a central issue in the Schrems II ruling and remains unresolved from a European adequacy perspective. The EU-US Data Privacy Framework attempts to address this through redress mechanisms, but legal challenges are ongoing. For CIOs handling sensitive personal data or business-critical intellectual property, reliance on US cloud services without additional technical safeguards (notably customer-controlled encryption) represents a residual sovereignty risk that no contract can fully eliminate. |

## 10. Stored Communications Act (SCA)

*Jurisdiction: UNITED STATES | Year: 1986 (Electronic Communications Privacy Act)*

| | |
|---|---|
| **What is it?** | The Stored Communications Act governs voluntary and compelled disclosure of stored electronic communications by service providers to government authorities. It establishes the legal framework under which US law enforcement can obtain access to emails, files, and data stored by cloud service providers through subpoenas, court orders, or warrants, depending on the nature of the content and its age. |
| **Obligations for companies** | Service providers subject to US jurisdiction must respond to lawful government requests for stored data. They may not voluntarily disclose content without legal process (with limited exceptions), but must comply with valid compelled process. Notification to the data owner is sometimes required but is frequently delayed or withheld under court order. |
| **Applicable to** | US-based service providers and cloud operators. Indirectly affects all organisations globally whose data is held by such providers, as their stored communications and files may be subject to compelled disclosure without their knowledge. |
| **CIO relevance: Digital Sovereignty** | While often overshadowed by the CLOUD Act, the SCA remains a significant access pathway for US domestic law enforcement. For CIOs, the practical implication is the same: data held by US providers in any jurisdiction may be accessible to US authorities. This underlines the importance of contractual notification clauses requiring providers to alert you (to the extent legally permitted) before disclosing your data, and of technical controls that reduce what is accessible to the provider. |

# UNITED KINGDOM — REGULATORY FRAMEWORKS

## 11. UK Data (Use & Access) Act 2025

*Jurisdiction: UNITED KINGDOM | Year: 2025*

| | |
|---|---|
| **What is it?** | The UK Data (Use & Access) Act 2025 is the post-Brexit UK reform of data protection and data governance law. It amends the UK GDPR and Data Protection Act 2018 to introduce a more flexible, risk-based approach to data use, establish a framework for data intermediaries and smart data schemes, and provide new rules on automated decision-making and digital verification services. It is intended to position the UK as a pro-innovation data economy while maintaining EU adequacy. |
| **Obligations for companies** | Organisations must comply with updated UK data protection rules, including revised legitimate interests assessments, updated automated decision-making provisions, and new requirements for transparency in data use. Organisations participating in smart data schemes gain specific rights and obligations around data sharing. The ICO gains enhanced enforcement powers. |
| **Applicable to** | All organisations processing personal data subject to UK jurisdiction, including non-UK organisations processing data of UK residents. Particularly relevant for organisations operating across both UK and EU markets, where dual compliance (UK GDPR and EU GDPR) is required. |
| **CIO relevance: Digital Sovereignty** | For Belgian CIOs with UK operations or customers, this Act adds a layer of dual compliance complexity. The UK is maintaining its own adequacy assessment track, and divergence from EU GDPR could eventually affect the current UK adequacy decision. CIOs should monitor whether UK reforms create compliance divergence that requires architectural changes in how personal data of UK versus EU data subjects is handled and stored. |

## 12. FCA PS21/3 & PRA SS1/21 (Operational Resilience)

*Jurisdiction: UNITED KINGDOM | Year: 2021 / implementation deadline March 2025*

| | |
|---|---|
| **What is it?** | PS21/3 (FCA Policy Statement) and SS1/21 (PRA Supervisory Statement) establish the UK financial regulators' operational resilience framework. Firms must identify their important business services, set impact tolerances for disruption, and demonstrate by March 2025 that they can remain within those tolerances during severe but plausible disruption scenarios. This directly regulates reliance on third-party and cloud services. |



ALLEGIANCE LAW

| | |
|---|---|
| **Obligations for companies** | Regulated firms must map their important business services to their underlying resources (including third-party IT and cloud services), stress-test their ability to continue within impact tolerances, and produce self-assessments. Boards are responsible for approving impact tolerances. Outsourcing arrangements must be assessed for their contribution to operational resilience or fragility. |
| **Applicable to** | UK-regulated financial services firms, banks, building societies, PRA-designated investment firms, insurers, and FCA-regulated firms with significant third-party dependencies. Firms with EU operations may also face parallel DORA requirements. |
| **CIO relevance: Digital Sovereignty** | For CIOs in UK financial services, this framework makes cloud provider dependency an explicit board-level risk topic. The emphasis on 'severe but plausible' disruption scenarios (including major cloud provider outages) means CIOs must have credible, tested continuity plans. Combined with DORA for EU entities, this creates a convergent international expectation: cloud resilience must be demonstrable, not assumed. |

## 13. Cyber Security & Resilience Bill (UK)

*Jurisdiction: UNITED KINGDOM | Year: Announced 2024 / legislation in progress 2025*

| | |
|---|---|
| **What is it?** | The UK Cyber Security and Resilience Bill is the UK's post-Brexit equivalent to NIS 2, expanding the scope of the existing NIS Regulations (2018) to cover a broader range of digital services, managed service providers, and supply chain participants. It aims to strengthen incident reporting requirements, extend regulatory scope to more sectors, and enhance the powers of regulators to investigate and enforce cybersecurity standards. |
| **Obligations for companies** | In-scope organisations will be required to implement security risk management measures, report significant cyber incidents to regulators within mandatory timeframes, and manage supply chain cyber risk. The Bill is expected to give regulators (including Ofcom and sector-specific bodies) stronger investigative and cost-recovery powers. |
| **Applicable to** | Expected to cover operators of essential services, digital service providers, and managed service providers operating in the UK. Organisations already subject to NIS Regulations (2018) should expect expanded obligations. The precise scope will be confirmed once legislation is enacted. |
| **CIO relevance: Digital Sovereignty** | For CIOs of organisations with UK operations, the Cyber Security & Resilience Bill signals regulatory convergence with the EU NIS 2 framework, but under UK jurisdiction and with UK-specific enforcement. Dual compliance planning is advisable now. Supply chain risk management, incident reporting capabilities, and board-level cybersecurity governance are the priority areas to strengthen in anticipation of the Bill's enactment. |

## 14. NIS Regulations 2018 (UK)

*Jurisdiction: UNITED KINGDOM | Year: 2018*

| | |
|---|---|
| **What is it?** | The UK Network and Information Systems (NIS) Regulations 2018 implemented the EU's original NIS Directive into UK law before Brexit. They impose cybersecurity and incident reporting obligations on Operators of Essential Services (OES) in sectors including energy, transport, health, digital infrastructure, and water, and on Digital Service Providers (DSPs) such as online marketplaces, search engines, and cloud computing services. |
| **Obligations for companies** | OES and DSPs must take appropriate and proportionate technical and organisational measures to manage security risks, prevent and minimise the impact of incidents, and notify the relevant competent authority of significant incidents without undue delay. The ICO is the lead supervisory authority for DSPs. Fines of up to £17 million are available for serious failings. |
| **Applicable to** | Operators of Essential Services (identified by competent authorities) and Digital Service Providers (cloud computing, online marketplaces, online search engines) established in or providing services into the UK. Post-Brexit, the UK NIS Regulations diverge from the EU NIS 2 Directive and will be updated by the Cyber Security & Resilience Bill. |
| **CIO relevance: Digital Sovereignty** | For CIOs with UK-based or UK-targeting operations, the NIS Regulations remain current law until the Cyber Security & Resilience Bill is enacted. Cloud service providers are explicitly in scope as DSPs. CIOs should ensure incident response plans include the UK notification |



ALLEGIANCE LAW

| | |
|---|---|
| | pathway to the ICO, and that supplier security assessments are documented. The imminent Bill will likely tighten and expand these obligations significantly. |

## 15. Telecommunications (Security) Act 2021 (UK)

*Jurisdiction: UNITED KINGDOM | Year: 2021*

| | |
|---|---|
| **What is it?** | The Telecommunications (Security) Act 2021 establishes a security framework for UK public telecommunications networks and services. It empowers Ofcom to set security requirements for telecoms providers, monitor compliance, and impose significant fines. It also provides the Secretary of State with powers to direct removal of high-risk vendors (notably used to mandate the removal of Huawei equipment from 5G networks) from critical telecoms infrastructure. |
| **Obligations for companies** | Public telecoms network and service providers must take appropriate and proportionate measures to identify and reduce security risks, manage the risk of using goods, services, or facilities from third-party suppliers, and ensure resilience of their networks. Providers must also comply with designated vendor directions issued by the Secretary of State. |
| **Applicable to** | Providers of public electronic communications networks and public electronic communications services in the UK. Applies to telecoms operators, internet service providers, and others operating UK telecoms infrastructure. |
| **CIO relevance: Digital Sovereignty** | While primarily aimed at telecoms operators, this Act is relevant for CIOs whose organisations operate their own communication infrastructure in the UK, or who rely on telecoms providers subject to these obligations. From a sovereignty perspective, it illustrates the UK's willingness to use supply chain security powers (including mandatory vendor removal) as a regulatory instrument. CIOs should understand which components of their UK communications infrastructure may be subject to designated vendor risk. |

# AUSTRALIA — REGULATORY FRAMEWORKS

## 16. Privacy Act 1988 (Australia)

*Jurisdiction: AUSTRALIA | Year: 1988 / amended 2022, 2024*

| | |
|---|---|
| **What is it?** | Australia's Privacy Act 1988 and its Australian Privacy Principles (APPs) govern the handling of personal information by Australian Government agencies and private sector organisations with an annual turnover above AUD 3 million. Major reforms enacted in 2022 and 2024 significantly increased penalties, expanded the definition of personal information, and introduced new provisions on automated decision-making, children's privacy, and cross-border data transfers. |
| **Obligations for companies** | Organisations must handle personal information in accordance with the APPs: collect only what is necessary, use and disclose only for the original purpose, maintain security, and provide individuals with access and correction rights. Cross-border transfers require reasonable steps to ensure overseas recipients comply with the APPs. Post-2024 reforms introduced enhanced penalties of up to AUD 50 million per serious interference with privacy. |
| **Applicable to** | Australian Government agencies and private sector organisations with annual turnover above AUD 3 million, plus certain smaller organisations (health service providers, registered political parties, credit reporting bodies). Extraterritorial reach applies to overseas entities 'carrying on business' in Australia. |
| **CIO relevance: Digital Sovereignty** | For CIOs of Australian organisations or multinationals with Australian operations, the significantly enhanced penalty regime demands attention. The cross-border transfer provisions directly implicate cloud sourcing decisions: reasonable steps must be taken to ensure overseas cloud providers and subprocessors handle personal information compliantly. The reform trajectory (towards stricter rules on automated decision-making and a right to explanation) signals increasing regulatory expectations that CIOs should anticipate in their AI and analytics governance. |



ALLEGIANCE LAW

## 17. Security of Critical Infrastructure Act 2018 (SOCI Act)

*Jurisdiction: AUSTRALIA | Year: 2018 / amended 2021, 2022*

| | |
|---|---|
| **What is it?** | The SOCI Act protects Australia's critical infrastructure from national security threats, including cyber attacks. Significant 2021 and 2022 amendments expanded its scope to cover 11 critical infrastructure sectors (including data storage and processing, cloud services, financial services, communications, and energy), introduced positive security obligations, and empowered the Australian Government to intervene in response to serious cyber incidents affecting national security. |
| **Obligations for companies** | Responsible entities for critical infrastructure assets must register assets with the Department of Home Affairs, report serious cyber incidents within 12 hours and other incidents within 72 hours, adopt and maintain a Critical Infrastructure Risk Management Programme, and comply with enhanced cyber security obligations. The Government may direct entities to take specific actions and, in extremis, directly intervene to manage a serious cyber incident. |
| **Applicable to** | Responsible entities for critical infrastructure assets across 11 sectors including data storage or processing, financial services, communications, energy, water, health, transport, defence, education, food, and space. Cloud service providers meeting asset thresholds are explicitly in scope. |
| **CIO relevance: Digital Sovereignty** | This is the most operationally demanding piece of Australian cyber legislation for large organisations. CIOs in regulated sectors must have a documented risk management programme, real-time incident detection capable of triggering 12-hour reporting, and board-level visibility of critical asset security posture. Cloud providers designated as critical assets face direct regulatory obligations. For Belgian CIOs managing Australian operations, understanding which assets trigger SOCI obligations (and what the Government intervention powers mean for operational control) is essential. |

### Key Takeaway for CIOs

Across all seventeen frameworks, one message is consistent: you cannot outsource accountability. Regulatory liability stays with your organisation regardless of what your vendor contracts say. The frameworks described in this memorandum are converging on a common expectation *i.e.,* CIOs can demonstrate, not merely assert, control over data access, supply chain risk, and operational resilience. Digital sovereignty is not a compliance checkbox. It is the organisational capability to remain in control of your critical assets, to change your mind about vendors, and to recover when things go wrong. That capability is built now, in contracts, in architecture, and in governance; not the moment of the incident.



ALLEGIANCE LAW

# ABOUT STEVEN DE SCHRIJVER

***"The only way to do great work is to love what you do"***

Steven is a partner at Allegiance Law and specializes in M&A, corporate law, IT and media, data protection and privacy and outsourcing.

Steven has more than 30 years of experience in advising Belgian and foreign companies on corporate transactions and has been involved in numerous national and cross-border transactions in the IT, media, telecoms and life sciences sectors.

Steven also advises some of the largest Belgian and foreign technology companies, as well as innovative entrepreneurs on complex commercial agreements and projects dealing with new technologies, most of the time with a cross-border element.

Steven has been involved in many IT, outsourcing, software and cloud application development, digital transformation, telecom/media projects (establishment of first mobile telephone operator in Belgium, acquisition of Flemish broadband cable operator, joint venture to launch video-on-demand services), outsourcing applicatinos, Software-As-A-Service, and cloud agreements on the customer side, and data protection (now: GDPR) compliance projects. He has a passion for artificial intelligence, robotics and drones.

He is also is active in the IBA Corporate and M&A Law Committee and the IBA Technology Law Committee and in ITechLaw. He is past-President of IFCLA and a member of the Tech M&A Committee of ITechLaw. He is Honorary member of AIJA and the Belgian member of EuroITCounsel.

Steven De Schrijver received in 20226 the Lexology Information Technology Lawyer of the Year, in 2023 (for the eight time) the Who's Who Legal award as Global Data Protection Lawyer of the Year and is considered a "Global Elite Thought Leader" in Data by Who's Who Legal (https://whoswholegal.com/steven-de-schrijver). Steven received in 2023 and 2024 also the Lexology Client Choice award for data protection and in 2012 the Lexology Client Choice Award for Corporate Law. Steven is recommended for corporate & M&A in Chambers, Legal 500 and IFLR and for IT law in Chambers, Legal 500 and Who's Who Legal.

Steven is known by his clients to go all the way to get the job done. He is pro-active, responsive, extremely available and pragmatic. Steven has an extensive international network of foreign lawyers with whom he closely cooperates on inbound and outbound cross-border transactions.

Let's connect on LinkedIn! https://www.linkedin.com/in/stevendeschrijver/

**Recent transactions:**

- Acquisition by Namsa of Medanex
- Acquisition by Archimed of Xpress Biologics
- Acquisition by Pixid, the French vendor management system-specialist, of TheMatchBox, a specialized text-mining company focused on the HR sector, primarily serving staffing agencies with AI search and matching services.
- Assistance of Pixid, with the acquisition of Connecting-Expertise, from the HR-group USG People Belgium.
- Acquisition by HypnoVR of Oncomfort
- Acquisition by NYSE-listed HubSpot of PieSync.
- DoubleVerify on its acquisition of Zentrick.
- Alpina Capital Partners on its acquisition of Objective International.
- Horizon Ventures on investment in Cloudalize.
- LivaNova on Belgian aspects of several global transactions.

**Relevant work IT:**

- DPG Media with the launch of streaming platform Streamz and the set-up, in this respect, of their joint-venture with Telenet.
- Radius Payment Solutions with launch of telecom activities in Belgium.
- ISS Facility Services, Mazda Logistics Europe on IT infrastructure and services outsourcing projects.
- Microsoft on its day-to-day commercial matters.



ALLEGIANCE LAW

## ABOUT ALLEGIANCE LAW

Allegiance Law is a Belgian independent law firm with offices in Brussels, boasting a strong team of lawyers with specialisations in areas including corporate, commercial, IT/IP/privacy, and EU regulatory (*e.g.,* artificial intelligence). Whether facing complex mergers, restructuring, or seeking to professionalise business operations, Allegiance Law tailors solutions by assembling specialised teams.

The firm supports national and international clients strategically by helping them to choose the best legal and financial structure for their business operations and transactions, transcending traditional methods and thinking outside the box. Allegiance Law's focus lies on IP and data-driven deals, of which the majority have a cross-border character. The firm operates regularly alongside among US, UK, French, Dutch, German and Swiss law firms, working seamlessly together. The team is specifically well equipped in the areas of technology, life sciences, media, advertising and entertainment, chemicals, transportation, and retail.

Our Areas of Expertise:

- Corporate Law and M&A
- Technology Law
- Commercial Law
- Privacy, Data Protection and Cybersecurity Law
- E-commerce and Digitalization Services
- Media, Gaming & Esports Law
- EU Regulatory
- Artificial Intelligence and Web3
- Life sciences
- Telecommunications
- Dispute Resolution and Mediation




ALLEGIANCE LAW