emma

Cloud Compliance · Q1 2026

The European Cloud Compliance Playbook

DORA, NIS2, and GDPR in Practice for Mid-Market Technology Leaders

> A reference guide for CISOs, DPOs, Heads of Compliance, CTOs, and CIOs navigating European cloud regulation. Structured for operational decisions, not legal theory.

Version 1.0 — March 2026

Table of Contents

Disclaimer: This playbook is published by emma and reflects the regulatory landscape as of Q1 2026. It is intended as practical guidance and does not constitute legal advice. Organizations should consult qualified legal counsel.

How to Use This Playbook

This is not a legal treatise. It is an operational reference guide — structured to help mid-market technology leaders translate European cloud regulation into infrastructure decisions, compliance workflows, and audit-ready evidence.

Each Chapter Follows the Same Structure

1 · What the regulation mandates — specific obligations in operational language
2 · Where mid-market companies most commonly fall short. Real-world gaps.
3 · What "good" looks like in practice. Concrete operational benchmarks
4 · How emma's capabilities map to specific requirements.

A Note on Regulatory Accuracy

Every regulatory reference cites specific articles, directives, or regulations. Enforcement dates, fine thresholds, and transposition statuses reflect the regulatory landscape as of Q1 2026. Where developments are proposed but not yet enacted, they are flagged explicitly as upcoming.

Who This Playbook Is For

SECURITY

CISOs & CSOs

Evaluating whether current cloud architecture meets regulatory security requirements across DORA, NIS2, and GDPR.

PRIVACY

DPOs & Privacy Officers

Mapping data protection obligations to cloud infrastructure controls, transfer mechanisms, and processor management.

COMPLIANCE

Heads of Compliance

Preparing for audits or building compliance frameworks from scratch with audit-ready evidence.

TECHNOLOGY

CTOs & CIOs

Making cloud architecture decisions with regulatory implications for mid-market companies (200–2,000 employees).

CHAPTER 1

GDPR

General Data Protection Regulation

CHAPTER 1

GDPR — Operational Cloud Implications

The General Data Protection Regulation (Regulation (EU) 2016/679) has been in force since May 2018, making it by far the most mature of the three regulations covered in this playbook. Its cloud implications, however, have sharpened considerably — particularly for international data transfers, sub-processor management, and the technical and organisational measures underpinning data security.

2,800+	€7.1B+	400/day
Fines issued since GDPR inception	Total fines levied through early 2026	Average breach notifications in 2025

Enforcement has broadened beyond big tech into financial services, healthcare, energy, and telecommunications. Cross-border cooperation between data protection authorities has become significantly more effective through the EDPB's coordination mechanisms. Most significantly for cloud operations, the largest fines in GDPR history have centred on international data transfer violations.

What makes GDPR different from DORA and NIS2 in the cloud context:

> DORA and NIS2 focus on ICT risk and operational resilience. GDPR focuses on the protection of personal data. The overlap is significant — all three require risk-based security measures, incident reporting, and third-party oversight — but GDPR adds specific obligations around data subject rights, lawful processing, data protection by design and by default, and international data transfers.

For cloud operations, GDPR's most consequential requirements are:

> Data processing agreements and sub-processor management, international data transfers, and technical and organisational measures.

GDPR · REQUIREMENT 1

Data Processing Agreements & Sub-Processor Management

What the regulation mandates:

Article 28 requires controllers to use only processors that provide "sufficient guarantees" for implementing appropriate technical and organisational measures. Processing must be governed by a Data Processing Agreement (DPA) that sets out the subject-matter, duration, nature and purpose of processing, type of personal data, categories of data subjects, and the obligations and rights of the controller.

The processor must not engage another processor (a sub-processor) without prior specific or general written authorisation from the controller. Where general authorisation is given, the processor must inform the controller of any intended changes concerning sub-processors.

Cloud operations implication:

Every cloud provider you use for processing personal data is a processor under GDPR. Their sub-contractors — including infrastructure providers, managed service partners, and support service providers — are sub-processors. You need DPAs with each, and you need visibility into the sub-processor chain.

Where mid-market companies most commonly fall short

Sub-processor chains are invisible

Most mid-market companies have DPAs with their primary cloud providers but lack visibility into the full sub-processor chain. When a cloud provider adds a new sub-processor, the obligation to review and potentially object falls on you.

DPA provisions do not reflect operational reality

DPAs often specify data processing locations at a high level ("European Economic Area") without granularity to specific countries or data centres. The DPA language may not match the infrastructure reality.

GDPR · REQUIREMENT 2

International Data Transfers

What the regulation mandates:

Personal data can only be transferred to a third country if the transfer meets one of the conditions in Chapter V. The primary mechanisms are adequacy decisions (Art. 45), Standard Contractual Clauses with a Transfer Impact Assessment (Art. 46), or specific derogations (Art. 49).

The EU-US Data Privacy Framework (DPF), adopted in July 2023, provides a new adequacy basis for transfers to certified US organisations. However, the DPF's durability remains subject to legal challenge.

Cloud operations implication:

Every cloud architecture decision that involves processing personal data outside the EEA triggers a transfer assessment. This includes not only where your data is stored, but also where it can be accessed from. The US CLOUD Act creates a specific compliance consideration for any personal data processed through US-headquartered cloud providers.

Where mid-market companies most commonly fall short

Transfer impact assessments are incomplete or absent

Many mid-market companies rely on SCCs without completing the Transfer Impact Assessment, particularly for cloud sub-processor transfers.

Access-from transfers are not assessed

A data transfer occurs not just when data moves to a third country, but also when it is accessed from one. Many assess storage locations but not access-from scenarios.

Reliance on a single adequacy mechanism

Companies relying entirely on the EU-US DPF have not prepared for a scenario where that framework is invalidated — as both Safe Harbor and Privacy Shield were before it.

GDPR · REQUIREMENT 3

Technical and Organisational Measures

What the regulation mandates:

Article 32 requires controllers and processors to implement technical and organisational measures appropriate to the risk, including pseudonymisation and encryption, ensuring ongoing confidentiality/integrity/availability/resilience, timely restoration of access after incidents, and regular testing of these measures.

Cloud operations implication:

Article 32 makes cloud infrastructure architecture and operational security controls a core component of GDPR compliance. Your cloud architecture — including redundancy, encryption, access controls, and monitoring — is itself a compliance measure.

How emma maps to GDPR cloud requirements

GDPR Requirement	Article(s)	emma Platform Capability
Data processing location transparency	Art. 28, 44–49	Granular location mapping; data residency policies enforceable at deployment time
Sub-processor visibility	Art. 28(2)–(4)	Multi-cloud provider management with visibility into provider services and geographic deployment
Data residency enforcement	Art. 44–49	Pre-provisioning guardrails blocking deployment to non-compliant regions
International transfer controls	Art. 44–49	Sovereign cloud provider integration; workload placement controls
Encryption and pseudonymisation	Art. 32(1)(a)	Encryption in transit and at rest; provider-native and external key management
Availability and resilience	Art. 32(1)(b)–(c)	Multi-cloud architecture with cross-provider redundancy and failover
Effectiveness testing	Art. 32(1)(d)	Continuous governance outputs; policy enforcement evidence

GDPR

GDPR Cloud Operations Self-Assessment Checklist

For each item, mark your status: ✅ In place · ⚠️ Partial/in progress · ❌ Gap identified

Data Processing Agreements & Sub-Processors

- [ ] DPAs in place with all cloud providers processing personal data
- [ ] DPAs specify data processing locations with sufficient granularity
- [ ] Sub-processor lists obtained from all cloud providers and reviewed
- [ ] Process in place to receive and evaluate sub-processor change notifications
- [ ] Sub-processor chains documented for audit purposes

International Data Transfers

- [ ] All personal data transfers to non-EEA countries identified and documented
- [ ] Transfer mechanisms (SCCs, adequacy decisions, DPF) identified per transfer
- [ ] Transfer Impact Assessments completed where SCCs are relied upon
- [ ] Access-from transfers assessed (support personnel, admin access from non-EEA countries)
- [ ] Contingency planning for adequacy mechanism changes documented
- [ ] Data residency controls enforced at infrastructure level, not just policy

Technical & Organisational Measures (Art. 32)

- [ ] Encryption in transit and at rest enforced across all cloud environments
- [ ] Access controls implemented consistently across all cloud providers
- [ ] Backup and recovery tested for personal data processing systems
- [ ] Monitoring and alerting operational across all cloud environments
- [ ] Effectiveness of technical/organisational measures assessed at least annually

CHAPTER 2

NIS2

Network and Information Security Directive 2

CHAPTER 2

NIS2 — Network and Information Security Directive 2

The NIS2 Directive (Directive (EU) 2022/2555) is the EU's updated framework for achieving a high common level of cybersecurity across member states. Unlike DORA, NIS2 is a directive that must be transposed into national law by each EU member state.

In May 2025, the European Commission issued reasoned opinions to 19 Member States for failing to notify full transposition by the deadline.

18	19	50+
Sectors covered across Annex I & II	Member States issued reasoned opinions (May 2025)	Employee threshold for scope (generally)

Relationship between NIS2 and DORA:

DORA is considered lex specialis in relation to NIS2 for financial entities. Financial entities covered by DORA apply DORA's provisions instead of equivalent NIS2 obligations. If your organisation is in financial services, DORA is your primary framework.

Penalties:

€10M	€7M	Art. 32–33
or 2% turnover — essential entities	or 1.4% turnover — important entities	Management disqualification possible

NIS2 · REQUIREMENT 1

Cybersecurity Risk Management Measures — Art. 21

Article 21 is the operational core of NIS2. It requires essential and important entities to take appropriate and proportionate measures to manage risks to their network and information systems.

Article 21(2) specifies ten minimum measures:

Risk analysis & IS security — documented policies covering all information systems including cloud.

Incident handling — procedures for preventing, detecting, analysing, containing, responding to, and recovering from incidents.

Business continuity — backup management, disaster recovery, and crisis management plans.

Supply chain security — assessing cybersecurity posture of suppliers and service providers.

Network & IS security — in acquisition, development, maintenance, including vulnerability handling.

Effectiveness assessment — policies to assess effectiveness of risk-management measures.

Cyber hygiene & training — for all staff; management body members specifically required.

Cryptography & encryption — policies regarding cryptography and encryption.

Access control & asset mgmt — HR security, access control policies, asset management.

Multi-factor authentication — or continuous authentication solutions where appropriate.

Where mid-market companies most commonly fall short

Supply chain security is the widest gap
Article 21(2)(d) requires entities to evaluate the cybersecurity posture of their suppliers and service providers. For cloud infrastructure, this means conducting structured assessments of your cloud providers' security practices — not just accepting their SOC 2 report, but evaluating their practices against your risk profile. Most mid-market companies rely on provider self-attestation without conducting proportionate independent assessment.

Effectiveness assessment is missing
Article 21(2)(f) requires policies and procedures to assess whether risk management measures are actually working. Many mid-market companies implement controls but have no systematic process for evaluating their effectiveness — particularly across multi-cloud environments where controls may be implemented differently per provider.

Management body accountability is not operationalised
Article 20 requires management bodies to approve and oversee Article 21 measures, and management members can be held personally liable. Most mid-market management teams have general awareness of cybersecurity risk but lack the structured engagement (training, decision documentation, regular reporting) that demonstrates accountability.

What "Good" Looks Like in Practice

Documented cybersecurity risk management policies covering all ten Article 21(2) measures, specifically addressing cloud infrastructure.

Supplier security assessments conducted for all cloud providers, proportionate to the criticality of the services they provide, and reviewed at least annually.

A defined process for assessing the effectiveness of risk management measures, producing evidence at least annually — including measures applied across cloud environments.

Management body training on cybersecurity risk documented and regularly refreshed. Management receives periodic reporting on cybersecurity posture, including cloud-specific risks.

Multi-factor authentication enforced across all cloud management consoles and critical systems.

How emma maps to Article 21 requirements

NIS2 Requirement	Art. 21(2)	emma Capability
Risk analysis and IS security policies	(a)	Unified governance across multi-cloud; policy enforcement as infrastructure configuration
Incident handling	(b)	Cross-provider monitoring and alerting; operational event correlation
Business continuity and DR	(c)	Multi-cloud workload orchestration; cross-provider failover; geographic redundancy
Supply chain security	(d)	Multi-provider governance framework; provider-level visibility into services and dependencies
Effectiveness assessment	(f)	Continuous governance outputs demonstrating policy enforcement state
Cryptography and encryption	(h)	Encryption in transit and at rest; provider-native and third-party key management
Access control and asset mgmt	(i)	Project-level IAM with least-privilege; automated asset discovery across environments
Multi-factor authentication	(j)	Platform access controls support MFA; enterprise identity provider integration

NIS2 · REQUIREMENT 2

Incident Reporting — Art. 23

Article 23 establishes a tiered incident reporting framework for essential and important entities. A "significant incident" is one that has caused or is capable of causing severe operational disruption or financial loss, or has affected or is capable of affecting other natural or legal persons by causing considerable damage.

Reporting timeline:

Early Warning — 24 Hours
Within 24 hours of becoming aware of a significant incident. Must indicate whether the incident is suspected of being caused by unlawful or malicious acts, and whether it could have a cross-border impact.

Incident Notification — 72 Hours
Updating the early warning with an initial assessment of severity and impact, including indicators of compromise where applicable.

Intermediate Report — On Request
Upon request by the CSIRT or competent authority. Must include relevant status updates on the handling of the incident.

Final Report — 1 Month
Detailing root cause, mitigation measures applied, cross-border impact, and the type of threat or root cause that likely triggered the incident.

Cloud operations implication:

The reporting obligation sits with the entity, not the provider. Your ability to detect and report provider-level incidents within the 24-hour early warning window depends entirely on your monitoring visibility across your cloud estate. Without cross-provider observability, you risk discovering incidents through customer impact rather than proactive detection.

Where mid-market companies most commonly fall short

Detection timelines exceed reporting windows
Many mid-market companies cannot reliably detect cloud-level incidents within timeframes that allow for a 24-hour early warning submission.

Incident classification criteria are undefined
Without pre-defined criteria for what constitutes a "significant incident" in their cloud environment, companies lose time on classification before reporting can begin.

Cross-border impact assessment is not operationalised
Few have mapped which cloud-hosted services, if disrupted, would have cross-border implications requiring flagging in the early warning.

emma relevance
emma's cross-provider monitoring and unified operational visibility enables faster incident detection across multi-cloud environments, supporting the 24-hour early warning requirement.

NIS2 · REQUIREMENT 3

Governance & Management Body Accountability — Art. 20

Article 20 establishes that the management bodies of essential and important entities must approve the cybersecurity risk-management measures taken by the entity, oversee their implementation, and can be held liable for infringements. This is one of NIS2's most significant innovations — it places personal accountability on senior leadership.

What the regulation mandates:

Management body members are required to follow training, and must ensure that training is offered to employees on a regular basis, in order to gain sufficient knowledge and skills to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

Approve cybersecurity measures
Management bodies must formally approve the cybersecurity risk-management measures adopted under Article 21.

Oversee implementation
Ongoing oversight responsibility — not a one-time approval but continuous governance of cybersecurity posture.

Personal liability
Member States must ensure that management body members can be held personally liable for infringements of Article 21.

Mandatory training
Management body members must undergo cybersecurity training; must also ensure regular training for all employees.

Cloud operations implication:

Board-level accountability means that cloud architecture decisions with cybersecurity implications — including provider selection, multi-cloud strategy, data residency, and resilience design — must be visible to and understood by management bodies. This requires translating technical cloud operations into governance-level reporting.

Where mid-market companies most commonly fall short

Governance is disconnected from infrastructure
Board-approved security policies exist as documents but are not operationally connected to cloud infrastructure decisions or enforcement.

Management body training is insufficient
Many organisations have not yet provided management body members with training that covers cloud-specific cybersecurity risks, multi-cloud dependencies, or the operational implications of NIS2.

NIS2

NIS2 Cloud Operations Self-Assessment Checklist

For each item, mark your status: ✅ In place · ⚠️ Partial/in progress · ❌ Gap identified

Cybersecurity Risk Management (Art. 21)

- [ ] Risk management policies documented for all ten Art. 21(2) measures
- [ ] Policies specifically address cloud infrastructure and multi-cloud environments
- [ ] Supplier security assessments conducted for all cloud providers
- [ ] Effectiveness of risk management measures is systematically assessed
- [ ] Incident handling procedures include cloud-specific scenarios
- [ ] Business continuity plans cover multi-cloud failure modes
- [ ] Vulnerability management and disclosure procedures documented and operational
- [ ] Cryptography and encryption policies documented and enforced
- [ ] Access control policies enforced across all cloud consoles and systems
- [ ] MFA enabled for all cloud management access
- [ ] Cybersecurity training programme in place for all staff

Incident Reporting (Art. 23)

- [ ] Significant incident criteria defined and applied to cloud environments
- [ ] Early warning capability within 24 hours of becoming aware
- [ ] Incident notification capability within 72 hours
- [ ] Cloud provider incidents integrated into entity-level reporting
- [ ] Final report process established with root cause analysis

Governance (Art. 20)

- [ ] Management body has formally approved cybersecurity risk management measures
- [ ] Management body receives regular reporting including cloud-specific risks
- [ ] Management body members have completed cybersecurity training (documented)
- [ ] Cloud architecture and provider decisions documented as governance decisions
- [ ] Accountability for cybersecurity oversight is clearly assigned

CHAPTER 3

DORA

Digital Operational Resilience Act

CHAPTER 3

DORA — Digital Operational Resilience Act

The Digital Operational Resilience Act (Regulation (EU) 2022/2554) is the EU's framework for ensuring that financial entities can withstand, respond to, and recover from ICT-related disruptions. It entered into application on 17 January 2025.

DORA is a directly applicable regulation — it takes effect across all EU member states without requiring national transposition. For financial entities, it is lex specialis to NIS2.

> **What makes DORA different:**
> DORA consolidates and strengthens requirements previously scattered across multiple EU directives and national regulations, replacing the patchwork with a single harmonised framework across 20 categories of financial entities.

1%	20	5
Daily worldwide turnover for critical ICT providers (up to 6 months)	Categories of financial entities in scope	Core pillars of DORA requirements

1 — ICT Risk Management
Sound, comprehensive, well-documented framework.
Art. 5–16

2 — Incident Reporting
Harmonised classification and tiered reporting.
Art. 17–23

3 — Resilience Testing
Vulnerability assessments, scenario testing, TLPT.
Art. 24–27

4 — Third-Party Risk
Register, concentration risk, exit strategies.
Art. 28–44

5 — Information Sharing
Voluntary cyber threat intelligence exchange.
Art. 45

DORA · PILLAR 1

ICT Risk Management Framework — Art. 5–16

DORA requires financial entities to maintain a "sound, comprehensive and well-documented" ICT risk management framework integrated into their overall risk management system.

Governance (Art. 5) — Management body must define, approve, oversee ICT risk management.

Framework & Strategy (Art. 6) — Documented, reviewed annually, subject to internal audit.

ICT Systems (Art. 7) — Reliable systems with sufficient capacity including peak demand.

Identification (Art. 8) — Identify, classify, document all ICT assets and dependencies.

Protection (Art. 9) — Access controls, authentication, patch management, encryption.

Detection (Art. 10) — Mechanisms to detect anomalous activities and incidents.

Response & Recovery (Art. 11) — Continuity policy and recovery plans, tested including cyber-attacks.

Backup (Art. 12) — Physically/logically separated; recovery tested periodically.

Learning (Art. 13) — Analyse vulnerabilities, threats, incidents; incorporate lessons learned.

Communication (Art. 14) — Plans covering incident responsibility and external disclosure.

Where mid-market companies most commonly fall short

Incomplete asset and dependency mapping

Most cannot produce a comprehensive dependency map across multi-cloud environments that satisfies auditor scrutiny.

Governance as documentation rather than operational practice

Board-approved policies exist as documents but are not operationally connected to infrastructure decisions.

Insufficient testing of backup and recovery

Companies test in isolation but have not tested cross-provider recovery or multi-cloud continuity scenarios.

How emma maps to DORA Pillar 1 — ICT Risk Management

DORA Requirement	Article	emma Capability
ICT asset identification & classification	Art. 8	Automated cross-cloud asset discovery; unified inventory across all providers
Protection & prevention	Art. 9	Policy-driven access controls; encryption enforcement; configuration guardrails
Detection of anomalous activities	Art. 10	Cross-provider monitoring; operational event correlation and alerting
Business continuity & recovery	Art. 11	Multi-cloud workload orchestration; cross-provider failover; geographic redundancy
Backup policies	Art. 12	Cross-cloud backup orchestration; physically separated recovery environments
Learning & evolving	Art. 13	Continuous governance outputs; policy enforcement trend analysis

DORA · PILLAR 2

ICT Incident Reporting — Art. 17–23

DORA establishes a harmonised incident classification and reporting framework. Financial entities must classify ICT-related incidents using criteria defined by the ESAs, and report major incidents to their competent authority.

Initial Notification — 4 Hours
Within 4 hours of classifying an incident as major (max 24h from detection).

Intermediate Report — 72 Hours
Updated assessment including severity, impact, and remediation status.

Final Report — 1 Month
Root cause analysis, total impact, and measures taken to prevent recurrence.

Voluntary significant cyber threat reporting
Entities may voluntarily notify competent authorities of significant cyber threats.

DORA · PILLAR 3

Digital Operational Resilience Testing — Art. 24–27

DORA requires financial entities to establish and maintain a comprehensive digital operational resilience testing programme as an integral part of their ICT risk management framework.

Two tiers of testing:

Tier 1 — All Entities

Vulnerability assessments and scans, open-source software analysis, network security assessments, gap analyses, physical security reviews, software compatibility reviews, source code reviews, scenario-based testing, performance testing.

Tier 2 — Significant Entities (TLPT)

Threat-Led Penetration Testing on live production systems at least every 3 years. Must cover critical or important functions, include ICT third-party providers in scope, and be conducted by qualified external testers aligned with TIBER-EU.

Where mid-market companies most commonly fall short

Testing does not include cloud provider dependencies
Many test their own applications but do not test the resilience of their cloud infrastructure layer or provider dependencies.

No cross-provider scenario testing
Few have tested scenarios where a primary cloud provider becomes unavailable and workloads must failover to an alternative provider.

TLPT readiness is low
Many entities that will be required to conduct TLPT have not yet identified which critical functions are in scope or how their cloud architecture maps to those functions.

DORA · PILLAR 4

ICT Third-Party Risk Management — Art. 28–44

Arguably DORA's most consequential pillar for cloud operations. It establishes comprehensive requirements for how financial entities manage risks from ICT third-party service providers.

General Principles (Art. 28)
Entities remain fully responsible for compliance regardless of what is outsourced. Must adopt a multi-vendor ICT strategy where feasible.

Register of Information (Art. 28(3))
Maintain a comprehensive register of all contractual arrangements with ICT providers.

Concentration Risk (Art. 29)
Assess whether arrangements would lead to concentration risk — evaluating substitutability and failure impact.

Key Contractual Provisions (Art. 30)
Contracts for critical functions must include: service descriptions, data locations, SLDs, incident assistance, monitoring rights, exit strategies.

Exit Strategies (Art. 28(8))
Must be comprehensive, documented, and periodically tested — ensuring termination without disruption.

Critical Provider Oversight (Art. 31–44)
ESAs will designate critical ICT providers for direct EU-level oversight. Non-compliance: up to 1% daily worldwide turnover for up to six months.

Where mid-market companies most commonly fall short

Register of information is incomplete
Many have a vendor list but not the structured, multi-level register the regulation requires.

Exit strategies do not exist or are untested
Few have completed architectural analysis, contractual assessment, and tested migration procedures for a genuine exit strategy.

How emma maps to DORA Pillar 4 — Third-Party Risk

DORA Requirement	Article	emma Capability
Multi-vendor ICT strategy	Art. 28	Native multi-cloud architecture; workload portability across 17+ providers
Register of information	Art. 28(3)	Unified provider registry with service, geographic, and dependency mapping
Concentration risk assessment	Art. 29	Cross-provider workload distribution visibility; substitutability analysis
Data location provisions	Art. 30	Granular data residency controls; deployment-time location enforcement
Exit strategies	Art. 28(8)	Workload portability; cross-cloud migration tooling; provider-agnostic orchestration
Sub-outsourcing oversight	Art. 29	Provider dependency mapping; sub-processor chain visibility

DORA · PILLAR 5

Information Sharing — Art. 45

DORA encourages (but does not mandate) financial entities to exchange cyber threat intelligence and information among themselves. This includes indicators of compromise, tactics, techniques, and procedures, as well as cybersecurity alerts and configuration tools.

Key requirements for information sharing arrangements:
Participation must be voluntary. Arrangements must protect commercially sensitive information, personal data, and competition law. Entities must notify competent authorities of their participation in information-sharing arrangements.

Cloud operations implication:
Multi-cloud visibility enables better threat detection and correlation across providers. emma's unified monitoring layer can support the identification of threats that may be relevant for information-sharing arrangements.

DORA

DORA Cloud Operations Self-Assessment Checklist

For each item, mark your status: ✅ In place · ⚠️ Partial/in progress · ❌ Gap identified

ICT Risk Management (Art. 5–16)

- [ ] Documented ICT risk management framework, reviewed within last 12 months
- [ ] Management body has formally approved and demonstrates active oversight
- [ ] Digital operational resilience strategy documented and linked to business objectives
- [ ] Complete inventory of all ICT assets, information assets, and ICT-supported business functions
- [ ] All dependencies between ICT assets and third-party providers mapped and documented
- [ ] ICT risk management framework subject to internal audit in the last 12 months
- [ ] ICT security policies cover access control, authentication, patch management, and encryption
- [ ] Continuous monitoring operational across all cloud environments
- [ ] ICT business continuity policy and response/recovery plans documented
- [ ] Backup and recovery tested including cross-provider scenarios
- [ ] Crisis management function established with defined communication procedures
- [ ] Communication plans documented including designated person for incident communications

Incident Reporting (Art. 17–23)

- [ ] Incident classification aligned with DORA criteria and ESA technical standards
- [ ] Incidents can be classified within hours of detection, not days
- [ ] Reporting workflow covers initial notification, intermediate report, and final report
- [ ] Cloud provider incidents integrated into entity-level incident management
- [ ] Post-incident analysis feeds back into the ICT risk management framework

Resilience Testing (Art. 24–27)

- [ ] Testing programme documented and reviewed annually
- [ ] Vulnerability assessments cover all cloud environments
- [ ] Scenario-based testing includes multi-cloud failure modes
- [ ] TLPT obligation assessed — conducted if applicable
- [ ] Contractual arrangements with cloud providers address testing participation
- [ ] Testing results documented and integrated into framework improvements

DORA · CHECKLIST (CONTINUED)

Third-Party Risk Management (Art. 28–44)

- [ ] Register of information covers all ICT service provider arrangements
- [ ] Register includes service descriptions, data locations, sub-contractors, and criticality assessments
- [ ] Concentration risk assessment documented for each significant provider
- [ ] Multi-vendor ICT strategy defined and linked to overall risk framework
- [ ] Contractual arrangements include Art. 30 provisions for critical/important functions
- [ ] Exit strategies documented, comprehensive, and tested
- [ ] Provider monitoring is continuous and produces evidence for supervisory review

CHAPTER 4

Convergence

Where the Three Regulations Overlap

CHAPTER 4

Where the Three Regulations Overlap

DORA, NIS2, and GDPR were developed independently but address overlapping risk domains. Many compliance obligations can be satisfied through the same operational controls — but only if designed with all three frameworks in mind.

Risk Management Frameworks

All three require documented, risk-based security measures — DORA (Art. 5–16), NIS2 (Art. 21), GDPR (Art. 32). A single comprehensive risk management framework addressing all three avoids duplication.

Incident Reporting

All three require incident reporting but with different triggers, timelines, and recipients. A single incident in a cloud environment may trigger reporting obligations under all three simultaneously.

Third-Party / Supply Chain Oversight

DORA requires a register of ICT providers. NIS2 requires supply chain security assessments. GDPR requires DPAs, sub-processor management, and TIAs. The underlying obligation is the same: you must know who your providers are, what they do, where they do it, and whether they meet compliance requirements.

What this means operationally:

Build once, map three times. Design your cloud governance, risk management, and incident response processes to satisfy the most demanding requirement across all three frameworks. Then map each process to its specific regulatory article in each regulation.

About emma

The cloud operations platform for distributed sovereign infrastructure

emma is built for organisations running distributed workloads across hybrid and multi-cloud environments — where operational complexity, unpredictable costs, and strict regulations get in the way of building.

It provides a single, policy-driven operating layer that spans hyperscalers, regional European cloud providers, AI-optimized infrastructure, and on-premises environments. From one dashboard, engineering, platform, and finance teams can deploy workloads, enforce compliance policies, and view and govern their entire infrastructure footprint. Sovereignty and compliance are built in through proactive guardrails, not bolted on.

With a vendor-neutral architecture, emma ensures organisations can choose the right infrastructure for cost, performance, and regulatory requirements — without lock-in or operational trade-offs.

Data Residency & Jurisdictional Control
Data stays within defined geographic and legal boundaries, enforced at the infrastructure layer across every environment.

Policy-Driven Workload Placement
Provider eligibility and sovereign constraints are maintained as infrastructure guardrails at deployment time.

Network Boundary Control
Cross-cloud data moves over emma's private networking backbone, reducing cross-border public routing exposure.

Continuous Governance & Compliance Evidence
Workloads continuously evaluated against GDPR, NIS2 and DORA policies. Audit-ready logs generated automatically.

Provider Portability & Exit Readiness
Tested migration paths across providers reduce concentration risk and meet regulatory exit capability requirements.

Encryption & Key Sovereignty
Encryption and key management policies enforced at deployment time. Organisations retain control over who holds the keys.

2021	15+	~90	NO
Founded & HQ in Luxembourg	Cloud providers supported	Cloud engineers at your service	US Cloud Act applicability

CERTIFICATIONS & FRAMEWORKS

emma operates under internationally recognized security and compliance frameworks, including ISO-certified security management and SOC 2 Type II audited controls, with data protection aligned to GDPR and resilience aligned with NIS2 and DORA.

APPENDIX A

Regulation Summary Table

	DORA	NIS2	GDPR
Legal instrument	Regulation (directly applicable)	Directive (requires transposition)	Regulation (directly applicable)
In force since	17 January 2025	Transposition deadline: 17 Oct 2024 (incomplete)	25 May 2018
Scope	Financial entities & ICT providers	Essential & important entities, 18 sectors	Any entity processing EU personal data
Risk management	Comprehensive ICT risk framework (Art. 5–16)	Ten minimum measures (Art. 21)	Appropriate technical & org measures (Art. 32)
Incident reporting	Major ICT incidents (Art. 17–23)	24h early warning, 72h notification (Art. 23)	Breach to authority within 72h (Art. 33–34)
Third-party	Register; concentration risk; exit (Art. 28–44)	Supply chain security (Art. 21(2)(d))	DPA; sub-processors; transfers (Art. 28, 44–49)
Max fines	National; 1% daily for critical ICT	€10M/2% (essential); €7M/1.4% (important)	€20M or 4% annual worldwide turnover

APPENDIX B

Upcoming Regulatory Developments

Initiative	Status (Q1 2026)	Relevance
EU Cloud and AI Development Act	Proposal scheduled Q1 2026	May introduce sovereign cloud standards and procurement criteria.
EUCS Certification Scheme	Under negotiation	May introduce EU-wide certification with sovereignty implications.
Cyber Resilience Act (CRA)	In force Dec 2024; full Dec 2027	Affects products with digital elements in cloud supply chains.
EU Data Act — Switching	Full ban on switching charges Jan 2027	Directly relevant to exit strategies and multi-cloud portability.

APPENDIX C

Glossary of Key Terms

Competent Authority
National authority designated to supervise and enforce a specific regulation.

Critical or Important Function (DORA)
A function whose disruption would materially impair the financial entity's performance.

CSIRT
Computer Security Incident Response Team — national entity receiving incident reports under NIS2.

DPA (Data Processing Agreement)
Contract required under GDPR Art. 28 between controller and processor.

ESAs (European Supervisory Authorities)
EBA, ESMA, EIOPA — the three EU-level financial supervisory bodies overseeing DORA.

Lex Specialis
Where a specific law and a general law overlap, the specific law takes precedence. DORA is lex specialis to NIS2.

Register of Information (DORA)
Comprehensive register of all contractual arrangements with ICT providers under Art. 28(3).

TLPT (Threat-Led Penetration Testing)
Advanced testing on live production systems against critical functions, required by DORA.

Transfer Impact Assessment (TIA)
Assessment required when relying on SCCs for international data transfers.

TIBER-EU
European framework for Threat Intelligence-Based Ethical Red-Teaming, aligned with DORA's TLPT.

> Build once, map three times. Design your cloud governance to satisfy the *most demanding requirement* across all three frameworks — then map each process to its *specific regulatory article.*

— The European Cloud Compliance Playbook, emma

Ready to Operationalise Cloud Compliance?

See how emma's unified cloud operations platform turns regulatory complexity into infrastructure-level controls.

BOOK A DEMO

Make Cloud Work for You

emma Technologies S.à r.l. · 19-21, route d'Arlon · 8009 Strassen · Luxembourg

emma.ms

info@emma.ms