The Privacy Control Framework

Operationalising GDPR and Data Governance in 2026

SURECLOUD®

www.surecloud.com

SURECLOUD®

GDPR Compliant

teiss Awards Winner Best Security Compliance Product

WINTER 2026 High Performer ENTERPRISE

SPRING 2026 Best Est. ROI ENTERPRISE

WINTER 2026 EMEA High Performer

Table of Contents

Highlights

- A five-domain Privacy Control Framework covering data visibility, risk assessment, governance and accountability, operational controls, and continuous monitoring
- Analysis of the 2026 enforcement environment, including the €1.2 billion in GDPR fines issued in 2025 and the €530 million TikTok decision, with the failure modes regulators are now consistently punishing
- Practical guidance on the overlap between GDPR and the EU AI Act, with a model for running them as one governance problem rather than two
- An ecosystem view covering AI systems, cloud and SaaS sprawl, and cross-border transfer risk, with control points mapped to each
- Programme metrics across coverage, responsiveness, risk reduction and operational efficiency, designed for board-level reporting

Who should read this?

This guide is designed for senior leaders responsible for privacy, data governance and information risk: Chief Privacy Officers, Data Protection Officers, General Counsel, Chief Information Security Officers, Chief Data Officers, and the audit, risk and board committee members who oversee them. It assumes familiarity with GDPR fundamentals and focuses on running privacy as an operational control framework at scale.

What this guide helps readers do

This guide helps readers assess where their privacy programme sits against the operating standard regulators now expect, identify the weaknesses that turn compliant organisations into enforcement targets, and adopt a five-domain control framework that joins privacy up with cyber risk, third party risk and enterprise governance. It covers what modern enforcement looks like, why post-2018 GDPR programmes drift, the Privacy Control Framework itself, the new ecosystem risks the 2018 model never anticipated, how to embed privacy into enterprise risk, what good technology enablement looks like, and the metrics that make privacy maturity defensible to a board.

Executive Summary

GDPR6 is eight years into enforcement. The question has changed.

In 2018, privacy leaders were asked whether their organisations were compliant. In 2026, they are asked something harder. Can the programme operate at scale as the data ecosystem keeps growing. Can controls keep up with cloud sprawl, new AI systems, longer sub processor chains, and the regulatory agenda building around them.

Enforcement has not softened. European supervisory authorities issued around €1.2 billion in GDPR fines during 20251, taking the cumulative total since 2018 past €7.1 billion across more than 2,800 enforcement actions12. More than 60 per cent of that cumulative value has landed since January 20232. Regulators are no longer focused only on big tech. Financial services, healthcare, telecoms and the public sector are now firmly in scope2.

The organisations that will manage the next three years well are the ones that have stopped treating privacy as a documentation exercise and started treating it as an operational control framework. Joined up with cyber risk, third party risk and enterprise governance. Measured. Reported to the board. Operated continuously.

The privacy landscape in 2026

Three forces are reshaping privacy governance. None of them are new. All of them have compounded.

Enforcement is sustained and widening

Regulators issued around €1.2 billion in GDPR fines in 2025, a figure closely matching 20241. Ireland's Data Protection Commission alone has now issued €4.04 billion in cumulative fines since GDPR took effect1, driven largely by the international data transfer cases concentrated in Dublin. Spain leads on volume, with 932 fines recorded, up 130 in the past year alone2. The common causes have not changed much: insufficient legal basis for processing, transparency failures, and inadequate security measures under GDPR Article 3226. What has changed is who receives them. Media and telecoms remain heavily exposed. Finance, healthcare, energy and the public sector are now routinely fined too2. Reported personal data breaches grew 22 per cent year on year, averaging 443 notifications across Europe every day1.

The EU AI Act has arrived alongside GDPR

General Purpose AI model obligations under Regulation (EU) 2024/1689 became applicable on 2 August 202537. The Act's high risk obligations under Annex III, and the enforcement powers of the AI Office, apply from 2 August 2026, with the remaining high risk obligations under Annex I following on 2 August 20273. Wherever an AI system processes personal data, the two regimes overlap. GDPR covers the lawful basis, transparency, data subject rights and security6. The AI Act adds obligations around risk management, documentation, human oversight, and post market monitoring for high risk systems7. Treating them as separate programmes will create gaps and duplicate work. Treating them as one governance problem will not.

The data ecosystem has outgrown the governance designed for it

When most organisations built their first GDPR programme, the data landscape was narrower. A handful of core systems, a known set of processors, a defensible inventory. In 2026 the picture is a sprawl of SaaS platforms, managed cloud services, machine learning tooling, and vendor sub processors who have their own vendor sub processors. Data flows that were documented once have drifted. The IBM Cost of a Data Breach Report 2025 places the global average cost of a breach at $4.44 million4, the first decline in five years, driven by faster detection and containment where it has happened. Much of the residual cost sits in the same weaknesses regulators punish: missing visibility, slow detection, unclear ownership.

The strategic implication is straightforward. The baseline that made organisations compliant in 2018 is not sufficient to keep them compliant in 2026.

Why GDPR programmes fail after initial compliance

Most GDPR enforcement actions do not punish organisations that never tried. They punish organisations that tried once, moved on, and stopped operating the programme. Five failure patterns recur.

1. Drifted inventories

Records of processing activities under GDPR Article 306 were written during the 2018 readiness push, often in spreadsheets or static documents. The business moved on. New systems came in. Old systems changed purpose. The inventory did not follow. A regulator asking what personal data you hold, where it is, and why, now hits a gap.

2. Manual privacy operations

Data protection impact assessments tracked in shared drives. Data subject access requests handled over email. Breach logs in a workbook only one person maintains. When volumes were low this was workable. Volumes are no longer low. The Information Commissioner's Office fined Advanced Computer Software Group £3.07 million in March 202511 after a ransomware attack compromised data belonging to 79,404 individuals. The ICO found failings against GDPR Articles 5(1)(f) and 32611: multi-factor authentication had not been deployed on the breached customer account, vulnerability scanning was incomplete, and patch management was inadequate. The pattern is not missing policies. It is missing operation.

3. Unclear ownership

The Data Protection Officer is often the only person with a full picture. Business unit heads do not know which processing activities they own, which vendors they are responsible for, or which DPIAs they should have commissioned. Accountability under GDPR Article 246 cannot sit in one corner office.

4. Shadow AI and shadow SaaS

Personal data is flowing into systems the privacy team has not seen. A team trials a generative AI tool on customer records. A department signs a SaaS contract that moves employee data to a new sub processor. Each looks minor in isolation. In aggregate they become the next breach.

5. Privacy run as a silo

The privacy programme reports separately from cyber, separately from third party risk, and separately from enterprise risk. A single incident can breach all three. A disconnected programme responds to it three times, slowly, in three different tools.

None of these failures are dramatic. They are the quiet kind that compound quarter after quarter until a supervisory authority asks a question the programme cannot answer.

Introducing the Privacy Control Framework

A Privacy Control Framework reframes GDPR obligations as five operating domains. Each domain has a defined purpose, a set of capabilities, and an explicit link to the wider governance programme. Together they move privacy from documentation to operation.

The framework is technology agnostic. It can be applied in financial services, healthcare, technology, or the public sector. It scales from a small privacy function to an enterprise programme. It is designed to be auditable.

Domain 1: Data visibility

Know what personal data you hold, where it lives, how it flows, and who touches it. Without this domain, every other control is theoretical. GDPR Article 306 requires records of processing activities as a minimum. Mature programmes go further.

Core capabilities:

- Living data inventories, maintained continuously, not reconstructed annually
- Data mapping across systems, business processes and data subjects
- Records of processing activities aligned to GDPR Article 30
- Sub processor and onward transfer registers with current status
- Data classification covering special category data, children's data and financial data

Domain 2: Risk assessment

Evaluate privacy risk continuously and in proportion. The GDPR Article 356 requirement for data protection impact assessments is a baseline. Modern programmes extend it to cover AI systems, new vendors, new jurisdictions and material changes to existing processing.

Core capabilities:

- DPIAs triggered by defined thresholds, not left to memory
- Privacy risk scoring aligned with the enterprise risk taxonomy
- AI impact assessments, integrated where AI processes personal data
- Data classification tied to downstream control requirements
- Transfer impact assessments for data leaving the jurisdiction, informed by Schrems II

Domain 3: Governance and accountability

Privacy cannot be owned by one office. GDPR Article 246 puts accountability on the controller as a whole. A governance model makes that workable.

Core capabilities:

- Clearly assigned ownership for every processing activity and every control
- A privacy policy framework with version control, approvals and expiry
- Board level reporting on privacy risk, incidents and regulatory change
- Integration with cyber, audit, third party risk and data governance committees
- Defined decision rights when privacy risk crosses risk appetite

Domain 4: Operational controls

The controls that actually protect personal data. These are the controls a regulator inspects during a breach investigation, as the Advanced Computer Software case demonstrated 11.

Core capabilities:

- Identity and access management, role based, reviewed on a cadence, with multi-factor authentication as the default
- Encryption in transit and at rest, with key ownership understood
- Data minimisation built into system design, not retrofitted, aligned to GDPR Article 25
- Retention management and automated deletion, aligned with documented retention schedules
- Consent and preference management, auditable across channels
- Operational workflows for data subject rights, meeting the one month window set out in GDPR Article 12(3)

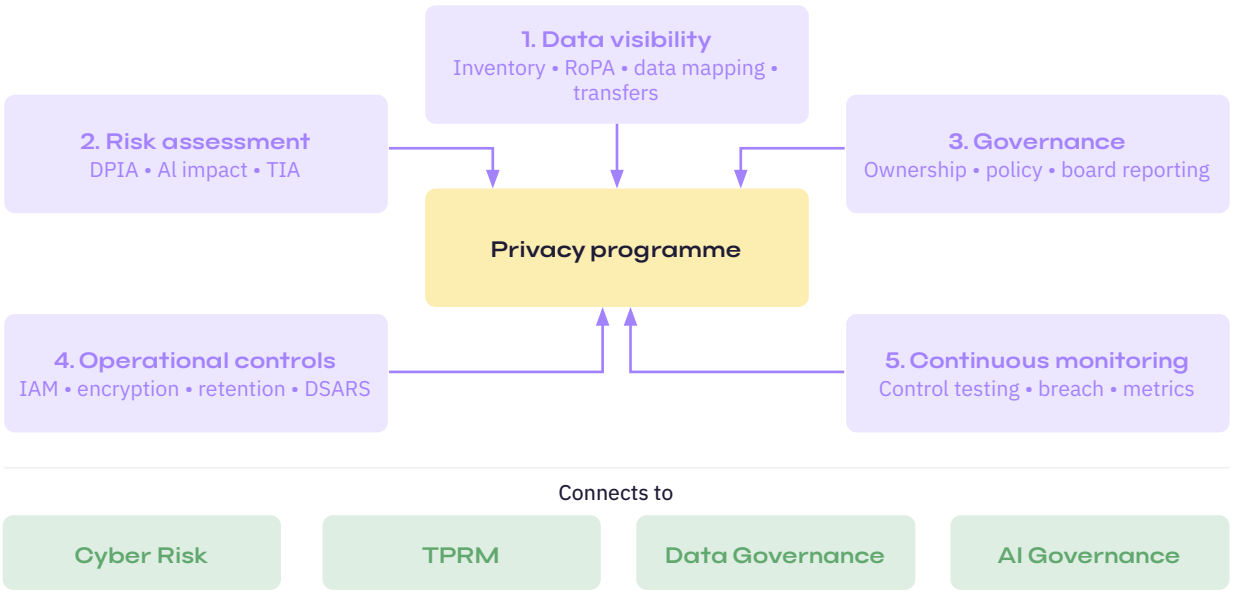
Domain 5: Continuous monitoring

A control that is not monitored is a control that has stopped working. Continuous monitoring is how privacy governance stays credible between audits.

Core capabilities:

- Automated control testing with evidence captured as part of the activity
- Incident and breach management with clocked notification workflows, meeting the 72 hour window under GDPR Article 33, operated in line with EDPB guidance on breach notification
- Regulatory change monitoring feeding into the control library
- Programme level metrics reported to the board
- Supervisory authority reporting ready to run, not assembled from scratch

The five domains interlock. Data visibility feeds risk assessment. Risk assessment drives operational controls. Governance sets ownership across all of them. Continuous monitoring closes the loop. Each domain is an anchor point into the wider programme: cyber risk, third party risk, data governance and AI governance.



Privacy risk in modern data ecosystems

Three ecosystem shifts have created risks the 2018 programme was never designed to cover.

AI systems processing personal data

AI is now the most material new source of privacy risk. Three specific exposures matter most.

Training data provenance. Models trained on scraped or repurposed personal data rarely meet GDPR Article 66 lawful basis requirements without substantial work. Special category data under GDPR Article 9 raises the bar further.

Model behaviour and data subject rights. A model that has memorised training data can leak it in output. A model that makes decisions affecting individuals triggers GDPR Article 226 obligations around automated decision making. Data subject rights of access, rectification and erasure apply to outputs, not just to inputs.

AI Act overlap. From 2 August 20263, AI systems that process personal data fall under both GDPR and Regulation (EU) 2024/16897. High risk systems carry documentation, risk management, human oversight and post market monitoring obligations that overlap directly with GDPR Articles 5, 25, 32 and 356. Running AI governance and privacy governance as separate programmes creates duplication and gaps. One programme with two lenses works better.

Cloud and SaaS platforms

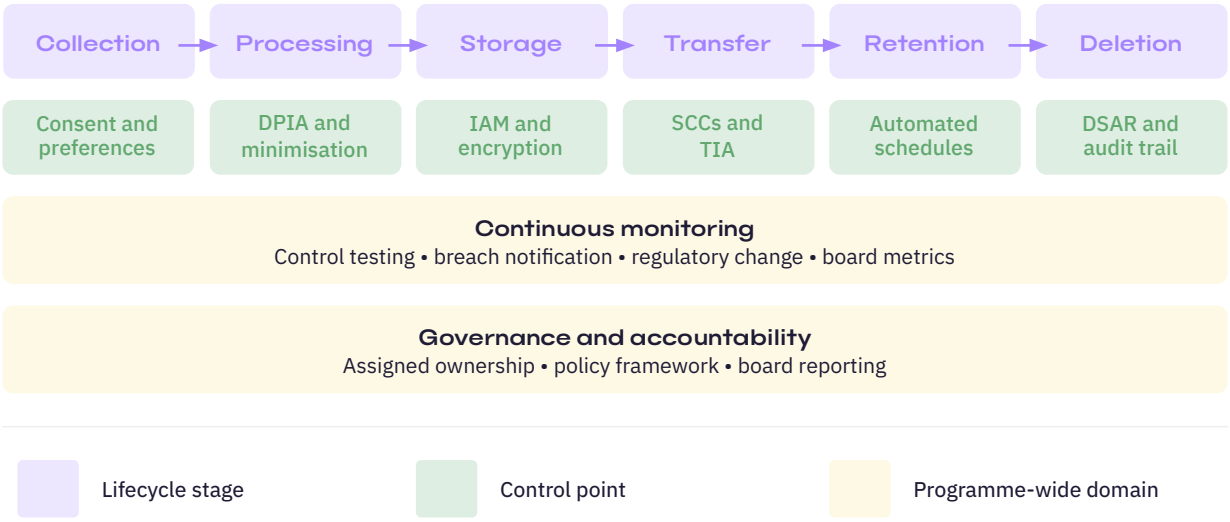
Personal data now sits in hundreds of cloud services. Each service has its own controls, its own sub processors, and its own configuration choices. Tenant misconfiguration is a common root cause in breach investigations. Encryption is often available but not enabled. Key ownership is often unclear. Transfer impact assessments, required under Schrems II5, are often done once during procurement and never revisited when the provider changes infrastructure.

Cloud platforms do not reduce privacy risk. They distribute it. The control framework has to follow the data.

Cross border transfers and sub processor chains

In May 2025 the Irish Data Protection Commission fined TikTok Technology Limited €530 million for unlawful transfers of EEA user data to China12. The fine broke down into €485 million for infringement of GDPR Article 46(1)612, concerning transfers to third countries without an adequate level of protection, and €45 million for transparency failings under GDPR Article 13(1)(f)612. During the inquiry TikTok informed the DPC that limited EEA user data had in fact been stored on servers in China, contradicting earlier statements to the regulator12.

The lessons for every organisation are not specific to TikTok. Schrems II5 obligations have not relaxed. Every vendor's vendor is part of the risk surface. Standard contractual clauses are necessary but not sufficient. Supplementary measures, transfer impact assessments, and continuous monitoring of sub processor changes all form part of the control framework.



Embedding privacy into enterprise risk management

Privacy stops being a corner office function when it uses the same risk language the rest of the business already speaks. The integration has four layers.

1. A shared risk register

Privacy risks scored on the same impact and likelihood scales as cyber, operational and financial risk. The board sees one register, not four. A risk that sits above appetite in privacy cannot be invisible in the enterprise view.

2. An integrated control library

Many privacy controls already exist in the cyber and compliance control library. Access management satisfies GDPR Article 326, ISO/IEC 27001:2022 Annex A, SOC 2 common criteria CC6, and elements of DORA operational resilience8 and the EU AI Act7 at the same time. Test the control once, map it to every obligation, evidence it once. The alternative is duplicated control testing and fatigue.

3. Board level reporting

Privacy metrics alongside cyber key risk indicators. Incident trends visible month on month. Regulatory change pipeline understood before it lands. Third party exposure quantified. A board that sees privacy quarterly makes different decisions from a board that hears about it when something goes wrong.

4. Joined up incident response

A data breach is simultaneously a privacy incident under GDPR Article 336, a cyber incident under existing security protocols, and often a vendor incident requiring third party notification. One workflow, three audiences, one audit trail.

The IBM Cost of a Data Breach Report 2025 places the global average breach cost at $4.44 million, down from $4.88 million in 20244. This is the first annual decline in five years, attributed to faster detection and containment, often driven by integrated security and privacy operations. Silos cost money. Integration saves it.

Technology as a privacy governance enabler

The Privacy Control Framework is technology agnostic. It is not technology optional.

Running data visibility, risk assessment, governance, operational controls and continuous monitoring on spreadsheets, shared drives and email is unsustainable at scale. Five enabling capabilities separate a platform that supports the framework from one that frustrates it.

1. Live data inventories: Automated discovery across systems. Classification aligned to regulatory categories. Live status rather than annual snapshot.
2. Workflow driven privacy operations: DPIAs, DSARs, breach notifications and vendor assessments run as tracked workflows with audit trails and clocked deadlines.
3. A shared control library: One control, multiple frameworks. Test once, satisfy GDPR, ISO 27001, SOC 2, DORA and AI Act obligations in parallel.
4. Continuous monitoring: Evidence captured as part of the operational activity, not retrofitted before an audit.
5. Regulator ready reporting: Supervisory authority submissions, board reports and assurance reports generated from the same data.

A platform that delivers these five capabilities operationalises the framework. A platform that does not will leave the programme relying on heroic effort from the privacy team.

Measuring privacy programme success

Privacy maturity is earned, not asserted. Meaningful measurement sits in four categories. The metrics below are the ones that answer board level questions without needing a translator.

Coverage

How much of the estate the programme actually covers.

- Percentage of systems with a current RoPA, refreshed within the last twelve months
- Percentage of processing activities with assigned owners
- Percentage of third parties with completed privacy assessments
- Percentage of high risk processing activities covered by a DPIA
- Percentage of AI systems processing personal data with a completed impact assessment

Responsiveness

How quickly the programme reacts when it has to.

- Median time to fulfil a data subject access request, against the one month window in GDPR Article 12(3)
- Median time to complete a DPIA
- Time from breach detection to supervisory authority notification, against the 72 hour requirement in GDPR Article 33
- Time from breach detection to affected data subject notification
- Backlog of open privacy risks

Risk reduction

The outcome metrics that demonstrate the programme is working.

- Year on year change in open privacy risks above appetite
- Incident frequency and severity trend
- Reduction in high risk audit findings
- Reduction in repeat findings

Operational efficiency

The internal metrics that keep the programme sustainable.

- Evidence collection effort per audit cycle
- Audit preparation time
- Control testing cadence and coverage
- Time spent on low value administrative work

Programmes that report on all four categories have something else in common. They make better investment cases. A board approves what it can measure.

The future of privacy governance

Four trends will shape the discipline over the next three years.

AI governance and privacy converge

The Act's main high risk obligations land on 2 August 2026, with a further tranche covering Annex I high risk systems following on 2 August 202737. Most high risk AI systems process personal data, bringing GDPR into every AI governance conversation. Organisations that run two programmes will find themselves repeating the same assessments, documentation and evidence. The ones running a single, joined up control framework will not.

Data sovereignty intensifies

Transfer rules have not relaxed since Schrems II5. Regional cloud, localisation requirements and sovereign infrastructure are becoming operational decisions rather than theoretical ones. The €530 million TikTok fine12 illustrates what sustained regulatory scrutiny of transfers now looks like. Expect transfer impact assessments to move from one off exercise to continuous control.

Continuous compliance replaces point in time audits

Supervisory authorities increasingly expect live evidence rather than annual snapshots. DORA8 requires continuous operational resilience testing for the financial sector. NIS29, transposed into member state law with a deadline of October 2024 and enforcement now active, expects similar evidencing for essential and important entities. The audit model is shifting.

Privacy becomes a board discipline

Privacy incidents reach the board anyway. The difference is whether they reach it as crises or as known risks being managed. Standing privacy metrics, alongside cyber key risk indicators, are becoming the norm in mature programmes.

Organisations that invest in operational privacy governance now will spend less of the next three years responding to surprises and more of it making deliberate decisions.

Conclusion

The organisations that will manage privacy regulation well over the next three years will not be the ones with the most policies. They will be the ones that have operationalised privacy governance as a continuous capability, joined up with cyber risk, third party risk and enterprise governance.

The Privacy Control Framework in this guide is a model for getting there. Five operating domains. One programme. Measured, reported and connected to the rest of the risk agenda.

Privacy stopped being a legal question some years ago. In 2026 it is an operational discipline and a board responsibility. Treat it accordingly.

References

1. DLA Piper. GDPR Fines and Data Breach Survey: January 2026.
2. CMS Legal Services EEIG. GDPR Enforcement Tracker Report 2024/2025: Numbers and Figures.
3. Future of Life Institute. EU AI Act: Implementation Timeline.
4. IBM Security. Cost of a Data Breach Report 2025.
5. Court of Justice of the European Union. Case C-311/18: Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II). Judgment of 16 July 2020.
6. European Parliament and Council of the European Union. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation).
7. European Parliament and Council of the European Union. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).
8. European Parliament and Council of the European Union. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA).
9. European Parliament and Council of the European Union. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity (NIS2 Directive).
10. European Data Protection Board. Guidelines 9/2022 on personal data breach notification under GDPR. Version 2.0, adopted 28 March 2023.
11. Information Commissioner's Office. Monetary Penalty Notice: Advanced Computer Software Group Limited.
12. Irish Data Protection Commission. Irish Data Protection Commission fines TikTok €530 million and orders corrective measures following Inquiry into transfers of EEA User Data to China.

For more information on how SureCloud can assist your organization, visit us online at **www.surecloud.com**, or email **sales@surecloud.com**

SureCloud Summary

SureCloud is the GRC platform that does more, better, with less. One platform covering risk, compliance, audit, third party risk management, business continuity and data privacy, powered by Gracie AI Agents with Personas and Skills, a virtual GRC team performing the activities the programme needs at scale. Founded in London in 2006, SureCloud has spent twenty years building GRC expertise into the platform. Customers include Specsavers, The Very Group, ICVE and Whitworth Bros.

Corporate Headquarters 1 Sherwood Street, London, W1D 7HR