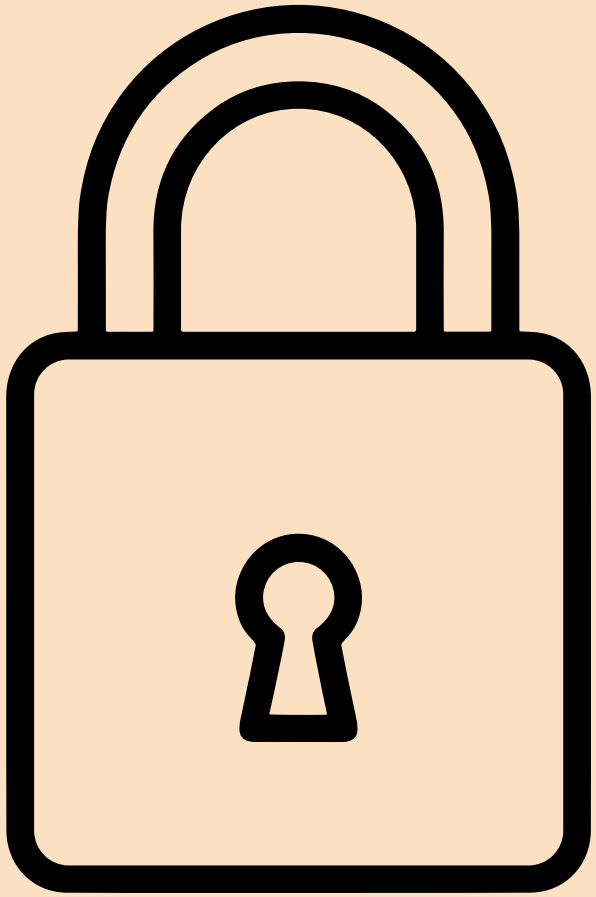
corestream grc

The practical guide to a proactive, always-on data privacy program



Introduction

From compliance to confidence

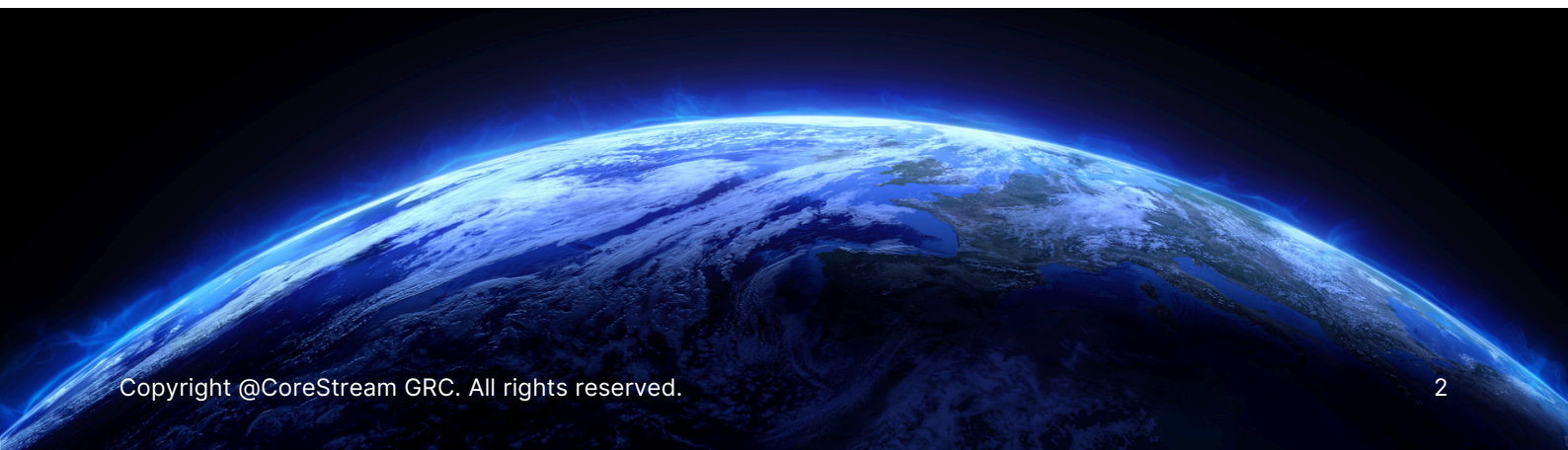
Most large organizations say they have privacy covered. And on paper, they do.

In practice, privacy often lives as **disconnected work**: documents, templates, and one-off reviews that prove something happened once, not a system that controls what happens next.

That gap matters because **privacy risk is created by change**. A new analytics use case. A vendor expansion. A "small" new purpose. A cross-border transfer that gets approved once, then **quietly grows as systems and suppliers evolve.**

When privacy goes wrong, it's rarely because a company has zero policies. It's because the organization cannot prove end-to-end that the way it **collected, used, shared, and retained personal data stayed lawful, consistent, and controlled as the business changed.**

If you fix that, you do not just **reduce risk. You move faster, with more confidence.** That's the competitive advantage.



Copyright @CoreStream GRC. All rights reserved.

What is Data Privacy?

In practice, “Data privacy” is how you **operationalize** that in day-to-day work, company-wide:

- who can **use** personal data
- for what **purpose**
- for how **long**
- who it can be **shared** with (including vendors and sub processors)
- what **approvals** and safeguards exist
- what **evidence** you can produce when someone asks, “show me”

If your program can’t answer those questions quickly, you’re managing privacy as paperwork.

Copyright @CoreStream GRC. All rights reserved.

Data privacy, also called information privacy, is an area of data protection that addresses the proper storage, access, retention, and security of sensitive data, which helps organizations meet regulatory requirements and protect the confidentiality and immutability of their data.

CROWDSTRIKE

An outdated model vs modern model of data privacy

An old model of data privacy lives within the privacy team and works off documentation.

What does this look like?

- policies that don't map back to real systems
- Data Protection Impact Assessments (DPIAs) completed once, then forgotten
- vendor questionnaires filed away in procurement
- privacy reviews that happen "around" projects, not inside delivery workflows
- evidence that something happened once, not that it stayed true over time

An **efficient**, modern data privacy strategy works off the operating model

What does this look like?

- clear decision points (when privacy must be assessed)
- named owners with authority to approve or block
- trigger-based reassessment when things change
- a single source of truth for processing, vendors, transfers, and controls
- an audit trail you can defend without scrambling across inboxes
- A variety of real-time dashboards/reports you can drill into to answer any questions thrown your way

Copyright @CoreStream GRC. All rights reserved.

Stop confusing privacy with security

A lot of organizations still treat data privacy as a branch of IT security. That approach produces “strong” programs on paper, but weak control in practice, because it optimizes for protecting systems, not governing decisions.

Here’s the clean separation that fixes the confusion:

Data security

- Data security is about **protecting data** from unauthorized access, loss, or compromise. Think encryption, patching, access controls, monitoring, incident response.

Data privacy

- Data privacy is about **lawful and fair use**. It governs whether you should collect or use personal data, for what purpose, for how long, and who you can share it with.

Data protection

- Data protection is often used as the umbrella term, especially in EU legal language, **covering both privacy and security**.

The key point: security is necessary, but it isn’t sufficient. You can secure data perfectly and still fail privacy if you use it for a purpose people didn’t agree to, didn’t expect, or that isn’t lawful in the first place.

That’s why “privacy programs” built around security controls and audit readiness often miss the real failure modes: purpose drift, uncontrolled sharing with vendors and sub-processors, retention creep, and weak accountability when the business changes.

Copyright @CoreStream GRC. All rights reserved.

The failure modes that keep showing up, according to senior leadership

Most enterprise privacy programs don't fail because they lack policies. They fail because the business changes faster than the governance.

So instead of trying to operationalize every principle in the book, focus on the ones that repeatedly drive real-world failure: **purpose control, third-party transparency, and accountability you can prove**.

1) Purpose limitation with real change control

Purpose limitation is where privacy stops being theory and becomes operational discipline.

You can collect data lawfully on day 1, then drift into unmanaged risk by day 30 because the use case expanded quietly.

Common flashpoints:

- Analytics and tracking expanding beyond the original scope
- AI model training, evaluation, and reuse of existing datasets
- Marketing segmentation and profiling creeping into "service" data
- Dataset merging across regions or business units that creates new inferences

What "good" looks like in practice:

- A defined trigger for a "purpose change" (not a reminder in a policy)
- A record of the approved purpose, linked to the system, dataset, and owner
- A workflow gate that forces reassessment before the new use goes live

Copyright @CoreStream GRC. All rights reserved.

2) Transparency and control across third parties

This is the supply chain reality your DPO team is already calling out:

> *"It's no longer just your organization's cybersecurity controls that matter. In your extended enterprise, your partners', vendors', and suppliers' vulnerabilities are now yours, too."*
>
> Paul Cadwallader
> GRC Strategy Director
>
> corestream grc

That's not just a mindset shift. It's what the breach data is showing: Verizon's 2025 reports **third-party involvement in breaches have doubled from 15% to 30%.**

2 points matter here:

1) People should **understand what you're doing with their data and why** (including legal basis and how to exercise rights).

2) You need the **same clarity when a vendor, supplier, or sub-processor touches that data.**

Where this breaks down:

- Third-party programs treated as "security-only"
- Vendor onboarding done once, then access expands and sub processors get added quietly
- The organization cannot answer, quickly and confidently:
  - Who has our personal data?
  - Where is it stored?
  - What are they allowed to do with it?

What "good" looks like:

- A **joined-up** privacy + third-party risk operating model (one system, not two programs)
- A **vendor inventory** that captures: what data, what purpose, where it sits, who can access it, and which sub processors are involved
- **Contract terms that match reality**: access limits, retention, incident response, cross-border transfer controls, end-of-contract handling

Copyright @CoreStream GRC. All rights reserved.

3) Accountability that survives change

Accountability is the principle most organizations claim, and the one most struggle to evidence.

You're not compliant because you said you are. You're compliant if you can show:

- **What decisions were made**
- **Who owned them**
- **What safeguards were applied**
- **What changed over time**

Where accountability fails in practice:

- One-time assessments mistaken for governance
  - A DPIA completed once, then never reopened when the system, vendor, or purpose changes
- Cross-border transfers expanding unnoticed
  - Vendors add sub processors
  - Hosting regions change
  - Access expands
  - Usage changes
  - The assessment becomes fiction if it never gets revisited

What "good" looks like:

- **Reassessment is trigger-based,** not calendar-based
- **Decisions and approvals are logged** in a way you can defend later
- **Evidence is connected to the work**, not scattered across inboxes

Copyright @CoreStream GRC. All rights reserved.

What value-based data privacy looks like at enterprise scale

If you want privacy that **holds up under scrutiny** aligned with your company's objectives, build an operating model around **decisions**.

1) Define the privacy decision points

These are the moments where privacy risk is created or changed:

- Launching a new product, app, or data feature
- Changing a processing purpose
- Onboarding a vendor that touches personal data
- Expanding vendor access (including new subcontractors)
- Moving data to a new region or cloud environment
- Introducing AI models or automated decisioning
- Changing retention rules or deletion processes

2) Assign real owners with authority

Privacy collapses when everything is "noted" and nobody can make the call.

A practical ownership model:

- **Low risk:** business owner + privacy guardrails
- **Medium risk:** privacy or legal review required
- **High risk:** exec owner sign-off (especially for sensitive data, large-scale processing, regulated environments, or cross-border transfers)

Copyright @CoreStream GRC. All rights reserved.

3) Make reassessment trigger-based, not calendar-based

Annual reviews are fine for housekeeping. They miss the real risk: change.

Trigger examples:

- New data categories collected
- New processing purpose
- New vendor or sub processor
- Material system change
- Incident, complaint, or regulator inquiry

4) Build your single source of truth

If you can't answer "where is our personal data, who has it, and why," you're guessing.

A strong program maintains:

- A data map (what, where, why, who touches it)
- An inventory of third parties and what data they handle
- Records of processing decisions and approvals
- Evidence of controls (not just policies)

A genuinely useful approach here is to document and visualize transfers, identify third countries and third parties, then prioritize review using a risk-based lens.

5) Bake privacy into third-party management

You need more than questionnaires. You need workflow integration.

Good practice includes:

- A centralized third-party inventory that spans the organization
- Extending data mapping beyond direct vendors into subcontractors (fourth parties)
- Workflows that scale based on data type and movement (not one-size-fits-all)
- Contract terms that align security, retention, access, incident response, and end-of-contract handling
- A practiced incident response plan that includes privacy, not just security

Want to learn more about embedding value-based GRC principles into your processes?

Download our value-based GRC guide

Copyright @CoreStream GRC. All rights reserved.

Cross-border transfers and TIAs in plain English

If you operate in the EU, or touch EU personal data.

The practical response many organizations adopted is embedding **Transfer Impact Assessments (TIAs)** into workflows, evaluating:

- The transfer tool (like SCCs)
- The receiving country's laws and practices
- Supplementary measures (technical, contractual, organizational)

Here's the line that matters:

If TIAs are a standalone document in a folder, they won't protect you.
If TIAs are a workflow gate tied to real transfers and vendor onboarding, they start to matter.

Copyright @CoreStream GRC. All rights reserved.

The role of technology in data privacy

Technology should do one job: reduce dependence on memory, email chains, and “we think we did that.”

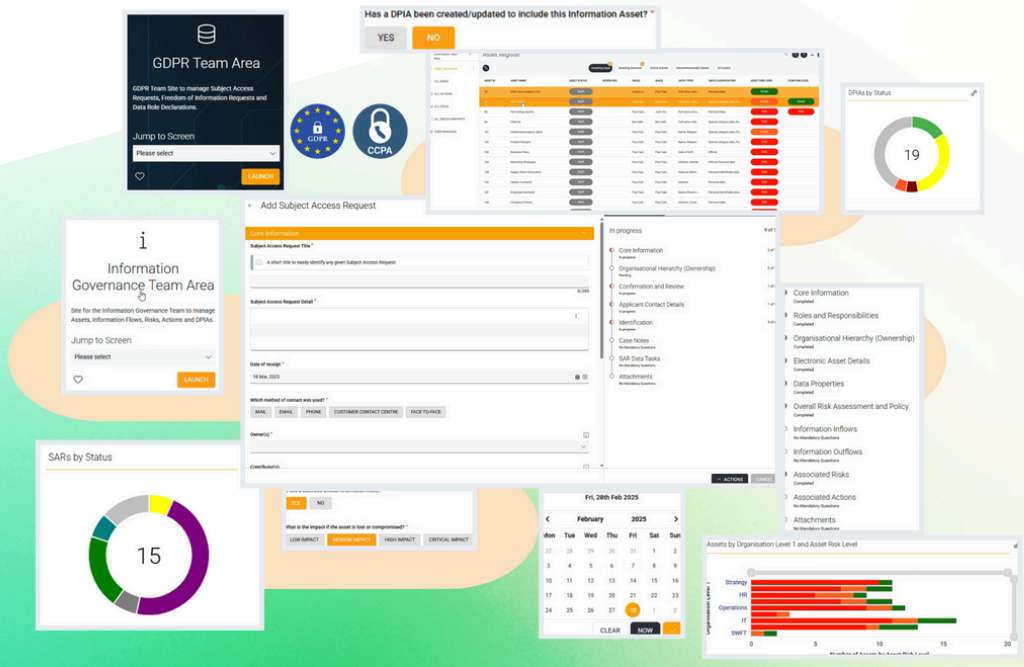
A useful privacy platform supports:

- **Continuous updates**, not one-time forms
- Clear **audit trails** for decisions and approvals
- **Integration** into vendor, procurement, and change workflows
- **Evidence capture** (controls, contracts, reviews connected to the system and process)
- Effective **dashboards** and reporting that give you that total picture of your privacy status across the organization

Here at CoreStream GRC we believe that **technology should be an enabler, not a barrier.**

Data Privacy solution

One warning: if your tool only digitizes questionnaires and report outputs, it will create nicer paperwork, not better privacy.



Copyright @CoreStream GRC. All rights reserved.

A practical self-check: do we have privacy capability or privacy paperwork?

If you can answer these cleanly, you're doing better than most organizations:

- Can we **list our highest-risk processing activities** and who owns them?
- Can we show when and why personal data is transferred cross-border, and what safeguards apply?
- Can we **prove what third parties touch** personal data, including subcontractors?
- When a purpose changes, do we have a **trigger that forces reassessment**?
- If a regulator asked "show me," could we **produce evidence** without scrambling across inboxes?

If the honest answer is "not really," that's not a moral failing. It just means your operating model is not built yet.

If you would like an audit of your current data privacy program, book in for one of our expert-led sessions.

In this 1-hour session, we will:

- Explore your current privacy processes
- Evaluate the effectiveness of your current strategy
- Identify a key focus for some quick wins
- Share insights and examples from our community of enterprises and their range of use cases
- Provide actionable takeaways to help mature your privacy program across a 12-month roadmap

Copyright @CoreStream GRC. All rights reserved.

axiom
corestream grc

For more information please contact:

Email us to book your demo:
demo@corestreamgrc.com

corestreamgrc.com

Book a workshop

Follow us on LinkedIn