Google Workspace

Assured Controls

Table of contents

01

Introduction

Collaboration fuels modern business. Sharing data across teams, regions, and organizations drives innovation, boosts team productivity, and accelerates business growth. Yet, this openness often collides with the demands of data security and compliance, creating a complex challenge for businesses to navigate.

The stakes are high. In 2024 alone, General Data Protection Regulation (GDPR) infringements in the EU resulted in 277 fines, totaling €1.19 billion[1]. High-profile cases like Meta's €1.2 billion fine[2] for transferring EU user data to the US without adequate safeguards underscores the financial and reputational risks of non-compliance.

At the heart of this challenge lies data sovereignty – the ability to control where your data is stored, how it's accessed, and who has the authority to handle it. With evolving regulations across regions like the EU, US, and others worldwide, maintaining sovereignty has become increasingly essential. Organizations must protect their data from unauthorized access while complying with a growing web of regional laws. This is a significant challenge for CIO, CISOs, and Compliance Officers, who often face internal resistance to data protection initiatives.

Assured Controls in Google Workspace provide organizations with the option to silo their data into regions, enabling organizations to choose where their data is processed and stored – such as the EU or US – to meet stringent regulations. With granular administrative controls, it helps to ensure your data remains protected from unauthorized access while empowering secure, seamless collaboration.

This guide offers a practical roadmap for safeguarding your data and meeting compliance challenges head-on. From assessing your current environment to implementing advanced controls, you'll gain the insights and tools needed to navigate the complexities of data sovereignty.

To achieve data sovereignty in a collaborative world, organizations must:

01 Control where their data is stored and processed.

02 Ensure that only authorized parties can access it.

Source: 1. https://www.enforcementtracker.com/?insights 2. https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

02

Rising tide of regulations

Governments worldwide are introducing stricter data protection laws to safeguard personal information and ensure local control over sensitive data. These frameworks are reshaping how businesses manage their information, creating new opportunities for compliance and innovation while raising the stakes for non-compliance.

European Union: GDPR and EU AI Act

The General Data Protection Regulation (GDPR) sets the global benchmark for data privacy. It mandates strict controls on how personal data is stored, processed, and transferred, especially outside the European Economic Area (EEA). Organizations must implement adequate safeguards, such as standard contractual clauses or equivalent protections, to ensure compliance. GDPR applies to businesses offering goods or services to EU citizens or monitoring their behavior, regardless of where the business is based.

The European Union Artificial Intelligence Act (EU AI Act) is the world's first legal framework for AI, regulating risk and fostering trustworthy use of AI in Europe. It applies to any business developing or deploying AI within the EU market, regardless of where they are based. AI systems are categorized into four risk levels:

Unacceptable risk

Banned AI applications that threaten safety and rights (e.g., social scoring, biometric surveillance).

High risk

AI in critical sectors (e.g., healthcare, law enforcement) must comply with strict regulations, including risk assessments and human oversight.

Transparency risk

AI systems, such as chatbots and generative AI, must clearly disclose AI-generated content.

Minimal or no risk

Low-risk AI (e.g., spam filters, AI-powered games) is not subject to restrictions.

United States: HIPAA, CCPA, and CDPA

While the U.S. lacks a unified federal data privacy law, sectoral and state-level regulations impose significant obligations:

HIPAA

Applies to healthcare providers, insurers, and their business associates, safeguarding patient information through strict privacy and security measures.

CCPA (California)

Grants consumers rights over their personal data, including the ability to access, delete, or opt out of its sale. It applies to businesses meeting specific revenue or data thresholds.

CDPA (Virginia)

Similar to CCPA, this law targets consumer privacy but emphasizes data minimization and transparency.

Asia-Pacific: APPI and PIPA

01 Japan’s Act on the Protection of Personal Information (APPI): Focuses on cross-border data transfers, requiring consent or equivalent protections when handling Japanese citizens’ data.

02 South Korea’s Personal Information Protection Act (PIPA): Enforces stringent requirements, including limitations on cross-border transfers and severe penalties for breaches.

South America: Brazil’s LGPD

Brazil’s Lei Geral de Proteção de Dados (LGPD) mirrors GDPR, demanding strict consent for data processing and heavy penalties for violations. It applies to businesses handling data related to Brazilian citizens.

Common challenges across frameworks

Despite regional differences, businesses face universal challenges.

These frameworks form the legal backbone of data sovereignty, but their implications are felt most acutely in industries handling sensitive data. Read on to explore how sectors like finance, healthcare, and technology navigate these unique challenges.

Cross-border complexities

Transferring data internationally requires compliance with multiple frameworks.

Evolving requirements

As laws like GDPR and LGPD continue to evolve, organizations must adapt to stay compliant.

Sectoral nuances

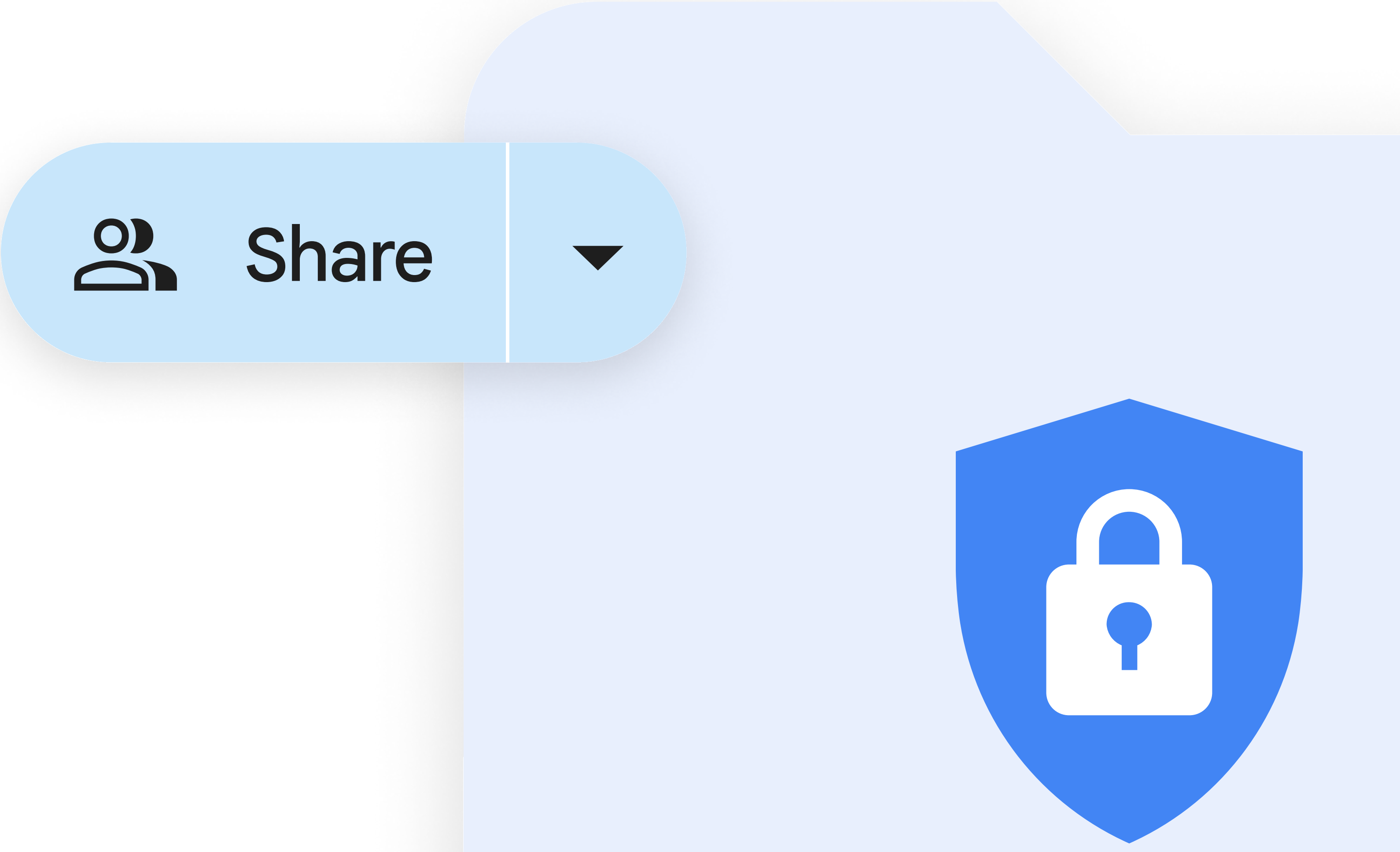
Regulations often overlap but vary in their application depending on industry-specific risks and needs.

03

Industries feeling the pressure

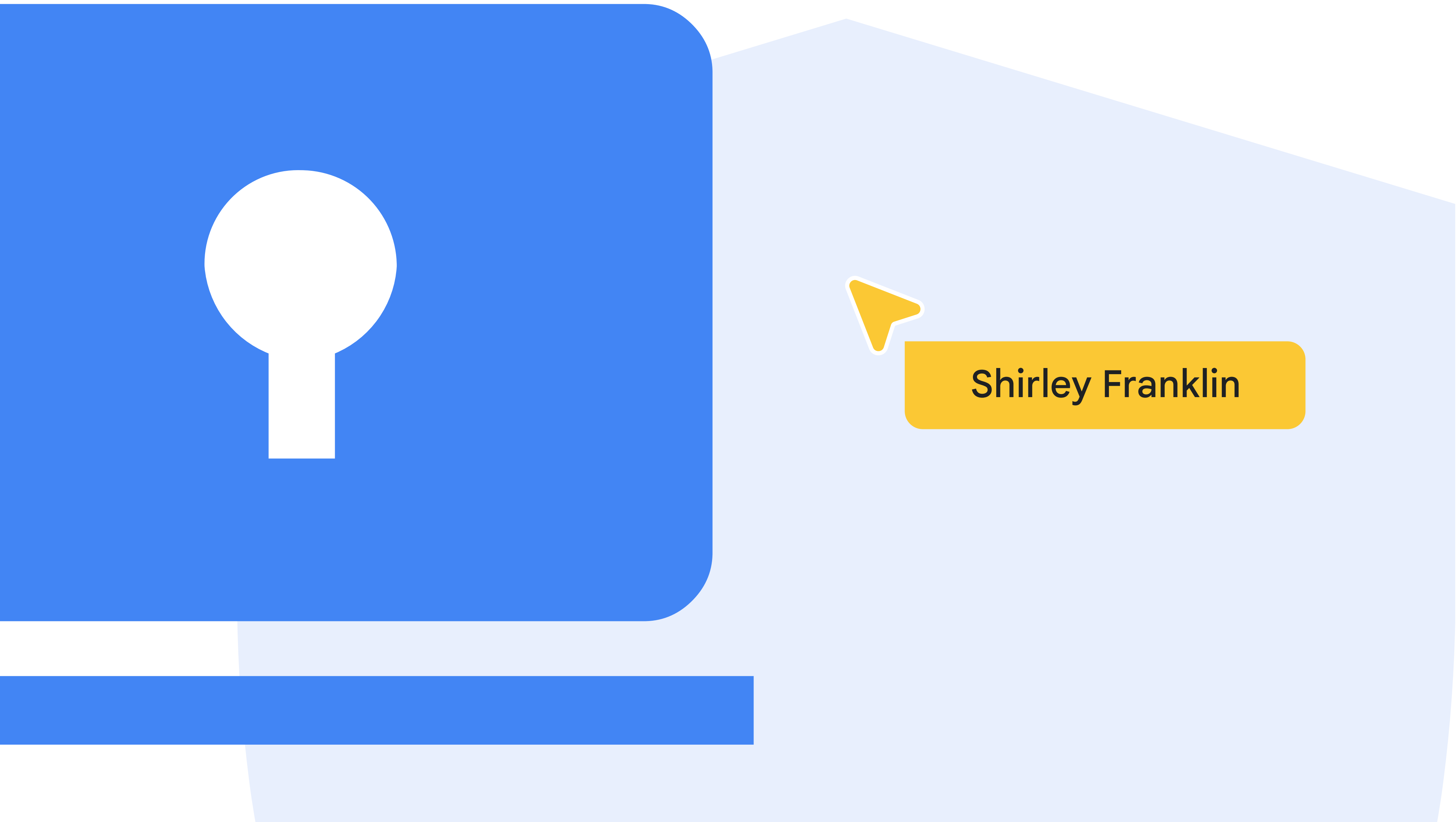
Data sovereignty challenges don't impact all industries the same way – they weigh more heavily on certain industries due to the sensitive data they handle and the rigorous regulations shaping their every move.

For sectors like finance, healthcare, government, and technology, achieving sovereignty isn’t just about ticking compliance boxes. It’s about protecting critical assets, building trust with stakeholders, and ensuring operations remain seamless and secure in an increasingly complex landscape.



Finance: Safeguarding trust in a competitive landscape

Financial institutions are under constant scrutiny due to the sensitive nature of customer data and their role in the global economy. Regulations like GDPR demand precise control over data storage and access, while Open Banking initiatives require sharing customer data securely with third-party providers to foster innovation.



Key considerations:

Cross-border challenges

Managing financial data across multiple jurisdictions introduces risks, especially when data flows between regions with differing regulatory requirements.

Legacy systems

Many banks rely on outdated infrastructure that complicates implementing modern compliance measures like advanced encryption or role-based access.

Reputational stakes

In an industry where trust is everything, a single breach or compliance failure can lead to significant financial and reputational damage.

By implementing solutions like granular access controls and localized data processing, financial organizations can confidently meet compliance standards while protecting customer trust.

Healthcare:
Balancing privacy with progress

In healthcare, patient privacy is both a legal obligation and an ethical commitment. The industry operates in a delicate balance – protecting sensitive medical records while enabling life-saving research collaborations.

Key considerations:

Regulatory overlap

Healthcare providers must navigate a complex web of regulations, from HIPAA in the US to GDPR in the EU, each with its own standards for data storage, encryption, and access.

Cross-border collaboration

Research institutions often require international data sharing, further complicating compliance. For instance, sharing anonymized patient data for global clinical trials must align with local data sovereignty laws.

Operational disruptions

Outdated systems and siloed data often lead to inefficiencies and increased risk during compliance audits.

Robust data protection measures, such as end-to-end encryption and real-time oversight tools, ensure healthcare organizations can meet compliance while fostering innovation and collaboration.

Government: Securing citizen trust and national security

Government entities manage vast amounts of sensitive citizen data, from tax records to national security information. The stakes are high – protecting this data is not only a compliance mandate but also a matter of public trust and national security.

Key considerations:

Geopolitical risks

Government agencies face unique challenges, including cyber threats and pressures from foreign actors, making data residency and sovereignty essential.

Transparency vs. security

Balancing openness with the need for stringent data controls is critical to maintaining public trust.

Regional laws

Government agencies must adhere to overlapping regulations like GDPR in Europe or local mandates that require data localization.

With data sovereignty tools such as end-to-end encryption and strict access controls, public sector organizations can secure their data without compromising transparency or operational efficiency.

Technology:
Innovating under scrutiny

Tech companies sit at the intersection of global scalability and regional compliance, processing vast amounts of user data across borders. For these organizations, data residency isn't just a compliance issue – it's critical for protecting intellectual property and maintaining customer trust.

"When data isn't regionalized or is handled by other technology providers, it's a risk for Europe, it's a risk for the nation, and it's a risk for Airbus. It's a risk that we can't afford."

Sebastien Aubineau, Airbus

Key considerations:

Global reach, local rules

Companies like Airbus highlight the importance of regionalized data processing to protect sensitive information and comply with sovereignty regulations.

Scalable solutions

Tech organizations must implement systems that allow them to expand globally without compromising compliance.

Emerging risks

Rapid innovation often leads to unforeseen vulnerabilities, from third-party application integrations to insufficiently controlled access.

Granular administrative controls and advanced security measures enable tech companies to navigate these challenges without stifling innovation or growth.

04 Five step plan

Navigating the path to data sovereignty requires a structured approach tailored to your unique needs, industry, and location. This guide outlines five actionable steps to help you take control of your data environment, comply with regulations, and build confidence in your organization's compliance strategy.

01

Assessing your environment

Understand where your data is stored, who has access, and which regulations apply. This is your starting point for identifying gaps.

02

Choosing data regions

Localize your data storage and processing to align with regulatory requirements while maintaining operational flexibility.

03

Refining access controls

Adjust permissions to ensure only the right people have access to the right data, minimizing exposure.

04

Strengthening data protection

Stay ahead of evolving cyber threats by enhancing your security measures and protecting sensitive data.

05

Reporting and oversight

Use ongoing monitoring and reporting to stay compliant and proactive in a constantly shifting regulatory environment.

01 Assessing your environment

Every journey begins with understanding where you are and where you want to go.

To navigate data sovereignty, start by understanding the external regulations that govern your industry and the internal realities of your data landscape. It's about aligning where your data is stored, how it's accessed, and what's required to meet compliance – while identifying gaps in your current setup.

Know the rules

Global frameworks like **GDPR**, **ISO**, and **SOC** set the stage for compliance. But these regulations don't exist in isolation – they demand alignment with your organization's specific operations:

GDPR (Europe)

Requires strict data residency within the European Economic Area (EEA) unless adequate safeguards, like standard contractual clauses, are in place. For organizations with European customers, understanding exactly where personal data is stored and transferred is critical.

EU AI Act (European Union)

Requires strict data residency within the European Economic Area (EEA) unless adequate safeguards, like standard contractual clauses, are in place. For organizations with European customers, understanding exactly where personal data is stored and transferred is critical.

DORA (European Union)

The Digital Operational Resilience Act sets technical standards to strengthen the IT security of financial institutions. Created by the European Supervisory Authorities (ESAs) and adopted by the European Commission, it unifies rules on operational resilience for the financial sector and ICT third-party providers.

SOC Compliance (United States)

Service Organization Control reports focus on trust principles such as security, availability, and confidentiality. Meeting these standards, established by the AICPA, requires rigorous internal audits and operational transparency, particularly for US-based organizations or those dealing with US entities.

ISO Standards (Global)

Offer globally recognized frameworks for managing information security, governed by the International Organization for Standardization. These standards are essential for multinational organizations operating in regions such as the EU, US, and Asia-Pacific to establish consistent security policies.

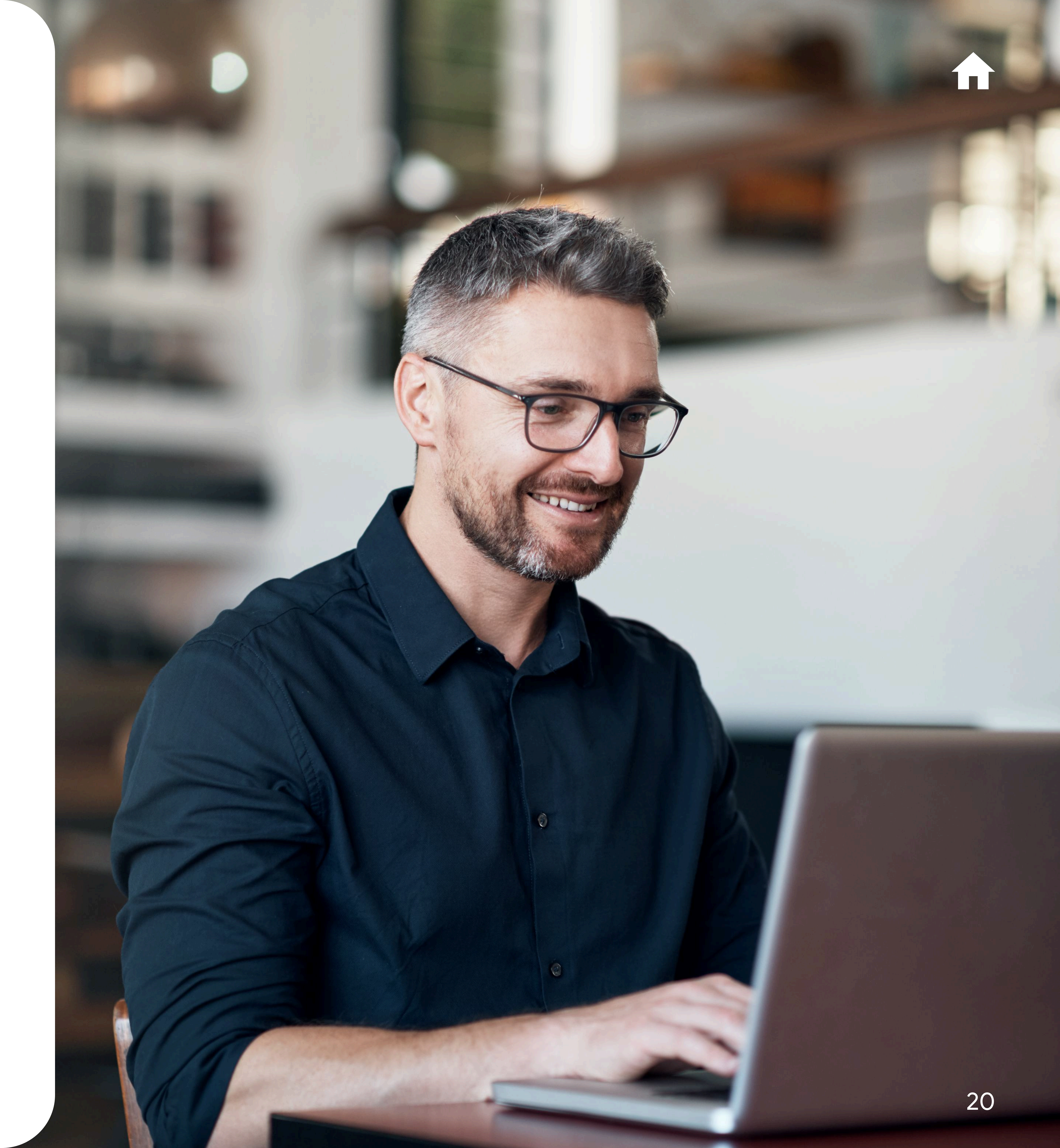
Audit Your Data

The next step is internal: map out your data environment. Where does your data reside? Who has access? What gaps exist in your current systems? Answering these questions is the foundation of your compliance strategy.

For instance:

- A healthcare provider may discover that sensitive patient data is stored across multiple cloud services, with varying levels of encryption. Cross-border data sharing for research further complicates compliance with GDPR (Europe) and HIPAA (United States).
- In this case, a data audit might reveal risks, such as unencrypted records or unclear access permissions, that must be addressed to meet regulatory requirements.

By aligning these insights with external regulations, organizations can bridge the gap between compliance mandates and operational realities.



Assemble your team

Data sovereignty isn't just a technical challenge – it's a collaborative one. Building the right cross-functional team is essential:

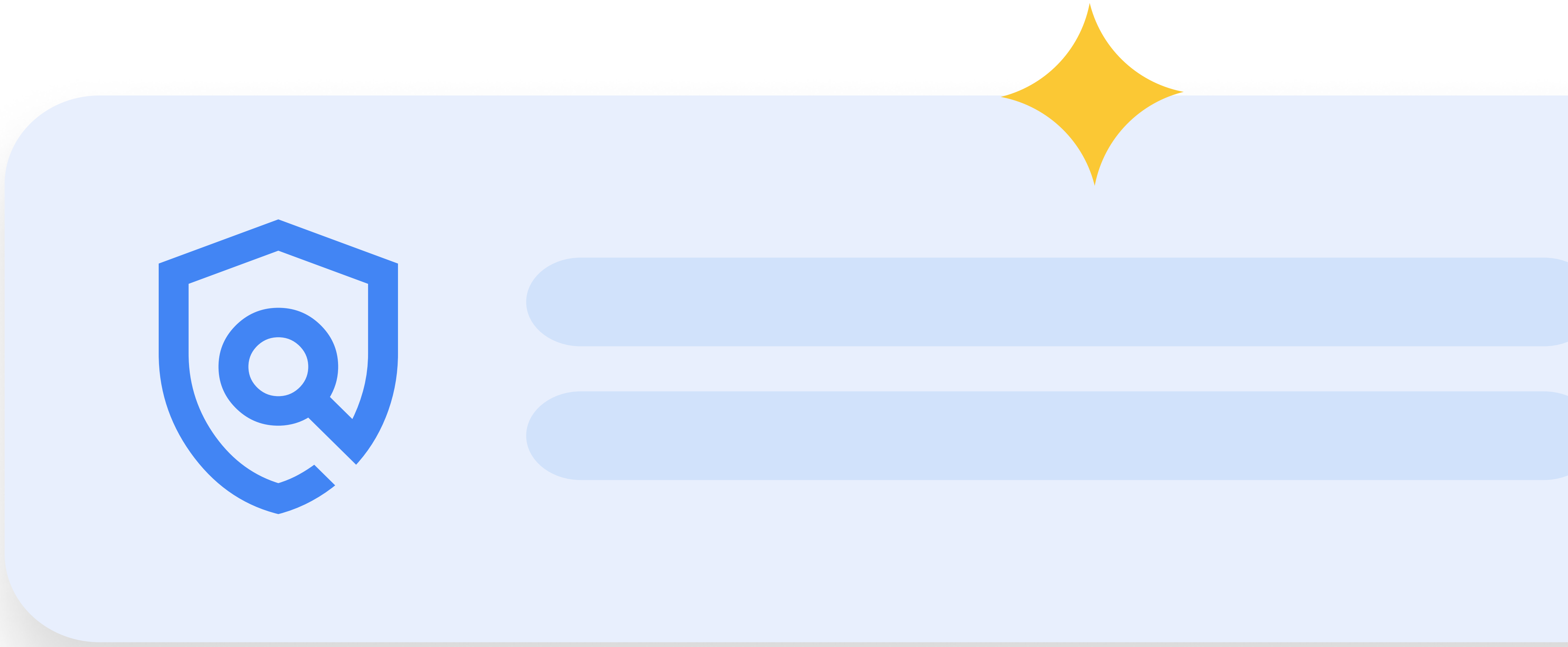
- **IT leaders** can map your technical infrastructure and address encryption or storage gaps.
- **Legal teams** can interpret regional regulatory requirements and ensure contracts reflect compliance needs.
- **Business units** can help identify practical impacts on day-to-day operations, like access permissions and workflow disruptions.

This team should work together to align your internal processes with the demands of frameworks like GDPR, SOC, or ISO in their respective regions.

Proactive Planning

Regulations evolve, and so do business needs – by taking these steps now, organizations can move beyond reactive compliance and build a framework that supports future growth.

For example, adopting solutions like **Assured Controls in Google Workspace** can provide a foundation for meeting data residency and access requirements, ensuring compliance while maintaining flexibility.



Data residency and access controls

02

Data residency isn't just about where your data lives – it's about ensuring you have control over how it's stored, accessed, and processed, while balancing performance, scalability, and compliance.

For organizations handling vast amounts of sensitive data, tools like Assured Controls in Google Workspace streamline compliance without disrupting operations.

> "We conducted an extensive analysis of in-region data processing, and it was a smooth process, mitigating the need for costly and complex third-party integrations. In addition, we haven't experienced any cases of malfunction or lagging – it's another day at the office without hiccups."
>
> Roman Spantgar, Product Owner Global Collaboration at Randstad

Local data residency vs. flexibility

The challenge for many organizations lies in striking the right balance between meeting strict residency requirements and maintaining operational agility. For example, organizations expanding globally often need to accommodate both regional regulations and performance demands.

This creates a common tension: how can organizations comply without building siloed systems that disrupt collaboration? Assured Controls in Google Workspace solves this by offering granular flexibility – you can define where your data is stored and processed while maintaining cloud scalability. For multinational businesses, this means the ability to set data residency policies for individual teams, departments, or regions without compromising performance.

Data processing: moving beyond storage

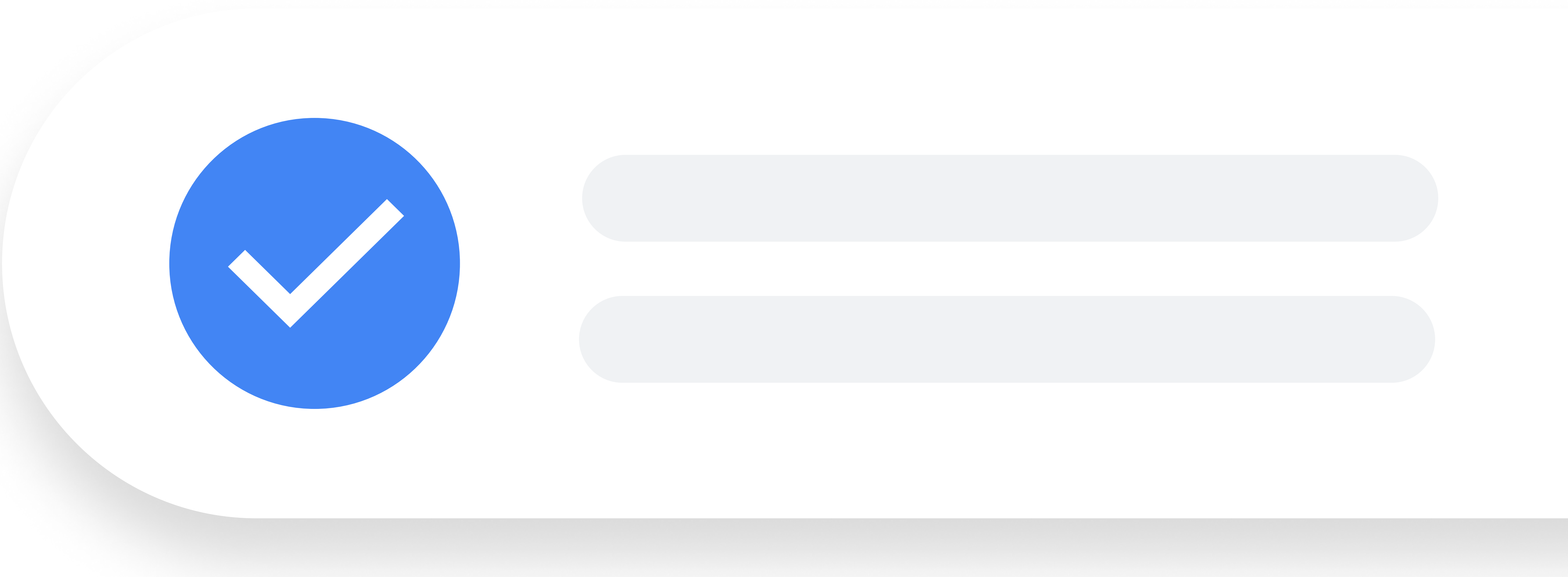
Many organizations focus heavily on where their data is stored but overlook where it's processed – a critical compliance factor in frameworks like GDPR. Data processing refers to how your data is used, analyzed, or shared, and often requires more oversight than simple storage. Assured Controls goes beyond storage alone. By enabling both storage and processing localization, it ensures organizations meet end-to-end sovereignty requirements.

Navigating U.S. healthcare compliance

Federal laws like HIPAA set nationwide standards for patient data protection, but state laws add complexity. Regulations like California's CCPA and Virginia's CDPA introduce stricter requirements around data privacy, consumer rights, and retention periods. Localized data processing helps healthcare providers navigate these overlapping mandates with confidence.

Future-proofing against regulatory changes

Data sovereignty is a moving target. Governments continue to refine existing regulations and introduce new ones, creating uncertainty for businesses. Rigid systems designed to meet today's rules may struggle to adapt tomorrow. Assured Controls in Google Workspace offers the flexibility to adjust data residency policies as regulations evolve. Whether that means migrating data across regions or refining access controls, the goal is to ensure your sovereignty posture keeps pace with change.



03 Refining access controls

Once your data is stored securely, the next step is ensuring that access is equally protected. By applying the principle of least privilege, organizations can ensure sensitive information is accessible only to those who truly need it. By tightening who can see what, organizations can reduce the risk of accidental leaks, internal misuse, and third-party vulnerabilities.

Why access controls matter

Unrestricted access to data is a growing risk in today's landscape. Internal over-permissioning increases exposure to leaks and errors, third-party access can complicate compliance, and regulations like GDPR, HIPAA, and other frameworks demand tighter oversight of who can access sensitive information.

How to refine access

The right tools help organizations enforce smarter, more secure access policies:

Zero trust frameworks

"Trust no one, verify everything" ensures every user, device, and connection is authenticated and authorized – even internal users.

Role-based access control (RBAC)

Aligning permissions to specific roles minimizes unnecessary exposure. For instance:

- Finance teams access payment systems, but not HR records.
- Healthcare providers see patient care data but not administrative files.
- Support teams access data only after explicit approval and for limited durations.

Access transparency and approvals

Implement workflows that require explicit authorization for third-party access. Tools like Access Approvals in Google Workspace ensure support teams only access data when absolutely necessary – with full visibility and control.

Client-side encryption

Adding another layer of security ensures businesses manage their own encryption keys, preventing even cloud providers from accessing sensitive data.

By implementing refined access controls, organizations can balance security and compliance with the demands of a collaborative, modern workplace. In the next step, we'll explore how strengthening your security measures can further reduce risk and ensure your organization stays ahead of evolving cyber threats.

Restricting access isn't just about security – it's about smarter operations.

Performance:
Storing data close to end users reduces latency, improves productivity, and ensures your teams can work seamlessly – no matter where they are.

Compliance:
Keeping data in-region avoids legal risks and ensures adherence to frameworks like GDPR, HIPAA, and other evolving regulations.

Security and Data Loss Prevention (DLP)

04

With data stored securely and access controls refined, the next critical step is protecting your organization against evolving threats. Assured Controls in Google Workspace provides advanced client-side encryption, granular access controls, and robust DLP (Data Loss Prevention) tools to make sure your data stays secure at every stage – whether it's in storage, in transit, or actively in use.

Why this matters

Modern organizations face increasingly complex security challenges:

- **External threats:** Phishing attacks, malware, and unauthorized access attempts are becoming more sophisticated. Organizations need proactive measures to defend sensitive information from bad actors.
- **Internal risks:** Over-permissioning, accidental sharing, and human error remain some of the leading causes of data breaches. Tightening access and embedding technical safeguards help mitigate these vulnerabilities.

The tools employees rely on every day – like browser extensions, productivity apps, or third-party integrations – can introduce unintentional vulnerabilities. Whether it's an unvetted app sharing sensitive data, overreaching permissions, or exposure to malicious software, these risks add an invisible layer of complexity to your security posture.

So how do you protect critical data while ensuring employees can work seamlessly with the tools they need?

With Assured Controls in Google Workspace, organizations gain a balance between flexibility and security:

- **Granular permissions:** Limit what third-party tools can access, ensuring sensitive data stays off-limits and reducing unnecessary exposure.
- **Client-side encryption:** Protect data end-to-end, even when employees collaborate across cloud services. Encryption ensures unauthorized apps or services can't read sensitive information.
- **Visibility and approvals:** Maintain oversight of which tools are being used, identify potential risks early, and approve external access only when it's truly necessary.

By embedding these controls, Assured Controls empowers organizations to give employees the freedom to innovate while keeping security front and center. Tools can stay helpful – not harmful.

Adding layers of defense

Assured Controls also integrates seamlessly with Zero Trust frameworks – adopting a "trust no one, verify everything" philosophy that requires every user, device, and connection to prove its credentials before accessing sensitive data.

Whether it's encrypting files before sharing or requiring multiple layers of approval for third-party access, these technical controls ensure that security is always proactive.

Why DLP matters

Data Loss Prevention (DLP) policies play a vital role in strengthening your security posture. They allow you to:

- **Monitor data movement:** Track sensitive data as it moves through your systems, identifying and addressing leaks or unauthorized sharing.
- **Set custom policies:** Define rules to automatically block, alert, or flag data sharing that violates compliance mandates.
- **Protect sensitive categories:** Identify and secure specific data types, such as personally identifiable information (PII), financial data, or intellectual property.

Security is often seen as a roadblock and an extra hurdle to collaboration. But in reality it helps businesses to operate confidently. With Assured Controls’ advanced encryption, proactive DLP policies, and approval processes, organizations can strike the right balance between protecting sensitive data and enabling collaboration.

In the next section, we’ll look at how reporting and oversight can help you stay proactive and compliant in an ever-changing regulatory environment.

Reporting and oversight: confidence through visibility

05

Data sovereignty doesn't stop once controls are in place – it's about proving those controls work. Reporting and oversight give organizations the ability to monitor, audit, and adapt their data strategies. With continuous visibility across encryption, access, and storage, you can ensure compliance isn't just achieved but maintained. For organizations like Randstad, real-time reporting tools simplify audits and ensure seamless compliance.

> "Implementing Data Regions has been a transformational step in evolving our strategy for personal data processing in the EU. It was a smooth process, and we haven't experienced any operational hiccups"
>
> Roman Spantgar, Product Owner Global Collaboration at Randstad

Think of reporting as a pyramid of control – a layered system that builds confidence at every level:

Client-side encryption:

At the base of your security is encryption. But encryption only works if it's applied consistently. Reporting tools confirm that sensitive data stays encrypted end-to-end, from creation to storage, while audit trails validate that encryption keys remain under your control.

Context-aware access:

Data access shouldn't just be controlled – it should be monitored. Real-time reporting surfaces anomalies, like unusual access locations, failed login attempts, or off-hours activity. This visibility allows you to address risks before they become incidents.

Granular access controls:

Oversight tools help you see who has access to what, when, and why.
By generating clear access logs and reports, you can identify over-permissioned roles, monitor temporary access (e.g., for support teams), and stay compliant with frameworks like GDPR and HIPAA.

Local data storage:

For industries under strict residency requirements, transparency is everything. Reporting tools verify that data remains stored where it's supposed to be – whether that's in a specific state or region – giving both your IT teams and regulators the proof they need.

Data regions:

Expanding into new markets? Reporting dashboards provide clarity on where data is stored, processed, and accessed, enabling businesses to adjust policies as regulations evolve or operations scale globally.

Zero-trust architecture:

Zero trust means never assuming – always verifying. Reporting tools log every access request, device, and user action, ensuring data policies are upheld while making it easier to monitor activity and detect suspicious patterns.

Why visibility matters

Without robust reporting, compliance can feel like a guessing game. Organizations need to prove they're meeting regulatory requirements while staying agile enough to respond to emerging threats. Assured Controls in Google Workspace provides the oversight tools you need to monitor, verify, and adapt your data strategy with confidence.

- **Simplify audits:** Generate compliance-ready reports aligned with frameworks like GDPR, HIPAA, and SOC 2. Assured Controls streamlines reporting for IT and compliance teams, offering detailed, auditable logs of all data activity at the click of a button.
- **Stay in control:** Real-time dashboards surface risks early, while transparent activity logs track every action, approval, or change. Teams gain the visibility needed to address risks, prove governance, and maintain trust.

With real-time insights, audit-ready reporting, and transparent activity logs, Assured Controls doesn't just help you meet compliance – it helps you stay ahead of it. By providing the tools to monitor, verify, and adapt, organizations can confidently demonstrate control over their data while reducing the risks of blind spots or evolving threats.

Strong reporting turns compliance from a checkbox exercise into a strategic advantage. With tools to monitor activity, verify controls, and respond proactively, organizations can confidently adapt to evolving risks and regulations while building trust.

05 Conclusion

Assured Controls in Google Workspace

can help organizations move much closer to achieving data sovereignty with minimal effort by combining advanced compliance tools with the flexibility and scalability of the cloud. It offers granular control over data storage, processing, and access while equipping businesses to adapt to evolving regulations. Whether safeguarding intellectual property in aerospace or managing sensitive customer data in finance, Assured Controls empowers organizations to focus on collaboration, growth, and innovation.

Learn more →