Flying Cloud®

Ready to *really* protect your data

EXECUTIVE BRIEFING

Surviving Global Data Sovereignty Regulation

5 Steps You Should Take to Gain Defensible Data Clarity and Protect Your Company

Takeaways

- China's PIPL and 100+ EU **data regulations** have global impact
- 83% of all **GDPR fines** have been levied against American companies
- AI models and data **multiply data risk** and compliance complexity
- **Businesses are accountable** for every data type and its behavior in any situation

Table of Contents

Compliance used to relate to how well your company protected personal, medical, or financial information from cybersecurity threats. Boy, how things have changed.

Massive proliferation of new data regulations is completely changing the compliance landscape. As of late 2025, 101 EU laws related to controlling digital assets and data have been adopted, with 24 more in process or in the planning stages[1]. China's Personal Information Protection Law (PIPL) similarly is aimed at protecting the data of Chinese citizens wherever they are. These regs affect businesses worldwide with both obvious, and more subtle, implications.

The EU and China data regs are more than a compliance challenge, although that's huge. The real issue is operational compatibility. Close alignment between regs makes it much easier for EU and Chinese companies to work together. Unless non-EU companies can document sovereignty compliance, they're at a significant competitive disadvantage.

In this paper, we'll summarize the EU and Chinese regulations, describe their potential impact, and show you why data security and governance are not enough. We'll also give you a roadmap and solution for gaining defensible data accountability to facilitate sovereignty compliance—quickly, easily, and with a documented chain of custody for every data binary.

[1] International Association of Privacy Professionals (IAPP) 2025 AI Governance Profession Survey
https://prod.iapp.org/media/pdf/resource_center/ai_governance_profession_report_2025.pdf

The Basics of Data Sovereignty

Under the concept of data sovereignty, data is connected to a physical location and subject to the laws of that area. But what does that practically mean? In some places, it's defined as data created or generated within a region. It has also been defined as data stored in a region. It can also mean data processed or used within a specific area. A single definition is...elusive.

It's pretty easy to regulate something that's born, lives, and dies within a defined geographic area. But data doesn't work that way. It's created or generated and shared, always moving and changing. Data is also treated differently depending on the context in which it's used. In a global economy, businesses have operations, partners, employees and digital connections all over the place. Data goes everywhere we want it to go without much thought. That's about to change.

For example, an international hotel group transferred the personal data of a Chinese citizen across borders to book his reservation at a European property and update his loyalty program membership. This ran afoul of PIPL. The Guangzhou Internet Court decided that it was legitimate for the citizen's data to cross borders for the purpose of booking a reservation, because it was necessary to satisfy performance of contract. However, simultaneously transferring the same data to the outside firm responsible for operating the hotel group's loyalty program was not legitimate. It required separate consent from the traveler. The hotel group's Customer Personal Data Protection Charter was not deemed sufficient consent. As a result, the hotel group was required to delete the citizen's private data, which caused him to lose his loyalty membership. It also required the group to partially compensate him for court costs.

Same data. Different context. The inability of the hotel group to control data behavior for two separate uses resulted in legal action and relatively small fines. It can get much worse.

What is data sovereignty according to the EU?

When planning your data sovereignty strategy, it helps to understand the philosophies behind them. In the EU, personal freedom and user privacy are considered fundamental rights when it comes to personal data. The General Data Protection Regulation (GDPR), effective since 2018, is based on the concept of individual rights, transparency, and accountability. Non-EU companies that handle the data of European citizens must comply or be fined.

Since GDPR, an explosion of new acts related to EU data and digital practices is creating a compliance nightmare. The EU's Digital Markets Act (DMA), Digital Services Act (DSA), AI Act, Data Governance Act, Data Act, Open Data Directive, the Network and Information Security Directive II, and the Cyber Resilience Act are just some of them. How do these play out in day-to-day business reality? That's for lawyers to answer, apparently. Add money to your legal budget.

For example, simply reading the objective of the EU Data Act (effective September 12, 2025) is confusing, to say the least. Theoretically, the EU is "freeing data" from restrictive vendor lock-in arrangements. But it's hard to see how a law designed to make data "more accessible and usable" achieves this by simultaneously dictating "who can use what data and under which conditions[2]."

The EU Data Act (and others) can apply to your business regardless of where you're headquartered. If your company falls into one of these three categories[3], you will likely face compliance obligations:

Hardware and software providers: If your company manufactures IoT devices, machinery, vehicles, wearables, or industrial sensors that reach EU markets or EU customers, the Data Act applies. This includes any products placed on the EU market through distributors or partners.

Data processing services: Cloud, SaaS, or PaaS services delivered to EU customers face switching and interoperability obligations. EU customers also require Master Service Agreements (MSAs) and Data Processing Agreements (DPAs) reflecting these requirements.

Supply chain participants: Even if you don't directly serve EU customers, the Data Act's "unfairness test" for data access terms applies through your supply chain, including distributors, OEMs, and integrators. If your products or services ultimately reach EU users through any supply chain, you can expect Data Act requirements to appear in your commercial agreements.

If you thought accounting for personally identifiable information (PII) was challenging enough, the Data Act applies to both personal and non-personal data, including relevant metadata. Think data generated by or from any connected device. Such regulated data even "includes data collected from a single sensor or a connected group of sensors, such as temperature, pressure, flow rate, audio, pH value, liquid level, position, acceleration or speed[4]." The data holder must have a contract with the user, defining their rights of usage.

[2] EU Data Act explained https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained
[3] https://www.fenwick.com/insights/publications/the-eu-data-act-what-u-s-tech-companies-need-to-know-about-the-eus-new-data-sharing-rules
[4] EU Data Act explained https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

This means businesses somehow have to account for almost every data type and its behavior in any situation.
When guilt is assumed and innocence must be proven, how can you prove you have, indeed, complied?

What if I don't comply?

If you're an American company, noncompliance paints a very large, very red target on your bottom line. The EU's fines on U.S. companies (particularly tech companies), just for alleged GDPR breaches, are brutal. Since GDPR took effect in May, 2018, as of March 2025:

- EU national data protection authorities have issued €5.65 billion in fines
- U.S. companies have been subject to 83% of those—€4.68 billion
- Second-ranking China has only paid €360 million
- All EU member states together only paid 9%—€529 million[5]

These fines are just for GDPR, and the EU shows no sign of easing up. Early in 2025, Italy's data protection agency issued a €15 million fine against OpenAI—20 times the company's revenue earned in Italy during the relevant timeframe.

Penalties for Data Act noncompliance are left to EU Member States. They're likely to impose GDPR-style penalties, in addition to retrieving any profits gained from noncompliance. Regulators and courts might also order other corrective actions.

How does China's PIPL differ?

Unlike the EU's stated insistence on personal freedom and user privacy, China's PIPL is focused on state control of personal data for national security. It gives governmental authorities greater access to data than the EU regulations, and it has stricter requirements for data localization. For companies outside of China, PIPL applies to data processing activities used to provide products or services to individuals in China and to data activities aimed at analyzing and evaluating citizens' behavior.

[5] Center for Data Innovation, April 17, 2025 https://datainnovation.org/2025/04/europes-gdpr-fines-against-us-firms-are-unfair-and-disproportionate/

Standard Contractual Clauses (SCCs)—These involve operational obligations and require detailed data mapping, strong contractual commitments from overseas data recipients, and demonstrable evidence of compliance. Importantly, the SCC mechanism is only available to data handlers not exceeding specific volume or sensitivity thresholds, and the contracts must be filed with the Cyberspace Administration of China (CAC) to become effective.

Non-compliance with these evolving regulations carries severe consequences. These can include:

- Fines up to 5% of annual revenue
- Operational disruptions
- Reputational damage
- Potential criminal liabilities for responsible officers
- Integration of PIPL violations into China's corporate social credit system, which can affect your ability to secure loans from Chinese banks, participate in public procurement projects, receive preferential tax treatment, or clear goods through customs efficiently.
- Being blacklisted and excluded from the Chinese market

How the EU and PIPL regulations align

The EU acts and PIPL have many similarities, and emerging regulations from other countries, such as India, will likely reflect many of the same requirements. For non-EU companies, particularly American companies, understanding these core similarities will make it easier to adapt your data strategies. Both, the EU acts and PIPL:

- Seek to control data at the point of origin
- Require documentation for movement
- Enforce cross-border approvals
- Treat data as a national resource
- Embed sovereignty directly into compliance
- Levy punitive fines for noncompliance

Let's talk about AI data

The EU's AI Act began taking effect in February, 2025, prohibiting certain uses of AI applications and emphasizing the importance of AI literacy. It applies to any business operating in the EU and non-EU companies that:

- Offer any AI system where the output can be used—or is intended for use—in the EU
- Sell AI technologies as part of a product or service integrated or sold by EU companies
- Have AI systems that process data concerning EU residents

The AI Act is too complex to summarize here, but gaining the same ability to identify, monitor, control, and enforce data movement and behavior will make it much easier to avoid infringement.

Why Data Security and Governance Are No Longer Enough

As the international hotel group discovered, it's going to take more than traditional data security measures to ensure they can safely operate within a confusing data sovereignty environment. It's not enough to know where data is stored, who has access rights, and which security measures are protecting the repository. It's not even enough to discover and classify data. Data sovereignty demands defensible data accountability and clarity. You must know your data's provenance, character, behavior, and usage. Preferably in real time.

How to achieve defensible data accountability?

The current regulatory posture recognizes potential problems and outlines consequences. There is little guidance on how to avoid issues. One thing is certain, data is at the heart of everything. Here are five steps every company should take to create a strong defense against data sovereignty challenges.

Good first steps are to:

1. Revisit your existing data standards

Businesses assume that data and their system processes are fine—most have no standards for data. Now, when you must be able to account for specific data, setting internal standards for data characteristics is essential. That's even more crucial with data destined for LLMs and AI processes.

Upgrade data management practices: Traditional data management practices are structured, rigid, and too slow for monitoring actual data behavior. Companies need the ability to track actual behavior of specific data binaries and quickly respond to anomalies in order to maintain sovereignty compliance.

Inventory data and its characteristics: Most enterprise data is collected in a host of formats and stored across multiple, diverse repositories and platforms. Companies don't know which data is in which formats or if it's relevant, complete, or even correct. Defensible accountability begins with data clarity.

Document data usage: You need to understand how your data is used by human users, and also by systems, across APIs, and in applications. How does it change, especially when influenced by AI processes?

Update standards: Today, "sensitive" data can mean just about anything. Any intellectual property, business process, financial data, IT data, programmatic binary data, or AI-related datasets and models that affect business performance should be considered sensitive to some degree. You'll need to know which specific data is under regulation and how it is allowed to behave, as well as how non-regulated data should perform.

2. Know your data

Traditional data discovery and classification tools are a start, but they don't go deep enough. You probably know what general kinds of data reside in repositories like an inventory management database, call center system, or product lifecycle management (PLM) system. Here's what you don't know:

Who created any specific file and when—the data's provenance. Was it created by a human, generated by a device, or synthesized by an AI algorithm?

Specific data content—including whether it's an entire original file or a composite of data from multiple original documents and creators. What's in the email body or header or attachment? Is there regulated content in an image, video, or audio file?

Who uses the data—which human users and systems handle the data?

How data is used—for what purposes, or in how many different contexts, is the same data needed? This is where the international hotel group infringed on PIPL regulations. The same data was used in multiple contexts with vastly different consequences.

Is the data qualifiable—is it accurate and complete? Database records, call logs, chat streams and other data might be missing fields or have wildly inconsistent formats. This is especially important for use in AI datasets.

What is the data's allowable use—where is it allowed to move? Who is allowed to have it, especially once it has left the original repository? What should be allowed to happen to it—whether it's acted on by people, other systems, devices, applications, or models?

Data discovery and classification are a start. But for AI and protecting your company against claims of data sovereignty infringement, everything hinges on being able to account for—and document—your data at a binary level.

3. Benchmark and track data behavior
In addition to knowing your data, you need to understand where it moves and how it behaves.

What's normal for a given piece of data? These are the questions you should be able to answer:

Where did the data go after leaving its original creation system? Should it stay within the enterprise network, workgroup, or specific application or is it normal to be sent to APIs or external websites?

Who or what used it? Who shared it? With whom was it shared? Are these allowable actions for this piece of data?

Which applications or systems normally receive or generate specific types of data? If customer data normally travels between a payment system and shipping application, great. If pieces of customer data in that process flow suddenly divert to an external website—that's an anomaly that should be investigated.

How does data move? Is it normal for data to travel between specific groups or users? What if data is suddenly downloaded and saved on a personal device, or the document title is changed and sent outside the company?

If data leaves your network, where does it go? When or how often? Who sends it?

What about data entering your network? Where is it coming from and who is receiving it? Is that normal behavior for your business process?

Data behavior is unique to your organization and it reveals far more than logs can reveal or classification can document. It can give you much deeper insight into usage context and business process integrity. Understanding normal data behavior also affords immediate visibility into potential cyber threats when data suddenly behaves in a way that's out of character for your organization. With the ability to monitor data behavior in real time, you can be alerted to anomalous behavior for rapid investigation and remediation.

4. Issue a data "passport" by assigning data policy
Your organization probably has cybersecurity policy assigned to systems for protections such as access control, threat detection, DLP, and phishing/malware quarantine. However, those policies don't apply to the data itself. With global data sovereignty regulation, individual data now needs its own "passport" for tracking, ensuring proper access and usage, and documentation.

Applying policy to individual data with granular specificity allows you to define:

- Who or what can access it, use it, and share it
- Where data is allowed to move, based on content instead of IP address
- Compliance with specific regulations to automatically ensure correct movement and usage
- Where it can't go

Using the international hotel group as the example again, they can apply policy to Chinese customer data that allows it to move freely within the group's Chinese network and only cross borders in cases that fulfill obligations of contract. The same data passport might also quarantine the data from other uses until specific consent agreements are obtained and the passport is updated. When a new Chinese citizen becomes a customer, the same policy can be automatically applied.

Policy also should be enforced automatically, so when a user or system causes data to behave outside of its defined permissions, the violation is alerted and action can be taken. Data policy makes data sovereignty compliance possible.

5. Document everything with a data chain of custody
If data policy makes compliance possible, chain-of-custody documentation makes your company defensible. Data has its passport "stamped" every time it moves or changes, automatically generating a chain of custody record for that piece of data. You can have digital proof of data accountability with a click.

We've Seen This Before

Flying Cloud delivers data sovereignty solutions based on 13 patents for data surveillance technology. Our enterprise-class solutions with multi-petabyte scale provide real-time data accountability on networks, in clouds, and across clouds. This is not the first time we've helped customers meet data sovereignty-style requirements.

We worked with a global manufacturing company to protect its IP and ensure compliance with China's State Administration for Market Regulation (SAMR) requirements. Using our CrowsNest® platform, the customer established appropriate geofencing for its data with zero trust security controls and chain-of-custody reporting. When summoned by Chinese compliance reviewers, the reporting was met initially with…silence. Finally, the official responded saying that they'd never seen anyone comply before. You can read about it **here**.

Today, when EU and Chinese data compliance requirements are aligning ever closer, sovereignty will become the default, not the exception. Flying Cloud CrowsNest gives you a single way to operate across global regulatory regimes without rearchitecting your worlds.

Issue Your Data's Passport

As an Oracle Cloud Infrastructure and Google Cloud Platform partner, we can help you quickly implement a sound data sovereignty strategy. Learn more about the CrowsNest Data Sovereignty solution. Even better, contact us, your sales representative, or Oracle or Google account representative to set up time with the Flying Cloud team.

For more information, request a meeting.
Or visit us at www.flyingcloudtech.com.