



eBook

# Navigating Data Privacy Laws

Where data  
& AI come to **LIFE**™



# Contents

|                                            |           |
|--------------------------------------------|-----------|
| <b>Introduction</b>                        | <b>3</b>  |
| <b>Data Privacy's Major Landmarks</b>      | <b>4</b>  |
| <b>Tracking Data Privacy Laws</b>          | <b>6</b>  |
| <b>Navigating to Data Privacy Maturity</b> | <b>8</b>  |
| <b>Questions About the Future</b>          | <b>10</b> |
| <b>How Technology Helps</b>                | <b>12</b> |
| <b>About Us</b>                            | <b>13</b> |



# Introduction

The legal and regulatory frameworks governing personal information continue to evolve. Even organizations with established privacy programs face new challenges as data privacy laws multiply and mature. Today's business and data leaders must navigate beyond basic compliance to ensure privacy across increasingly complex technology ecosystems while demonstrating measurable value.

This guide explores how organizations can elevate their approach with mature privacy programs, leverage intelligent data management solutions and transform privacy from a cost center to a strategic advantage.



# Data Privacy's Major Landmarks

**Advances in technology, emerging laws and regulations and growing public awareness all shift the landscape for the professionals who need to stay on top of data privacy. Consumers, companies and countries are vying for control over data.**

Staying informed about the issues that affect your organization and using this knowledge to drive responsible data management practices is crucial to ensuring compliance and keeping your data-driven business moving forward.

Here are eight landmark data privacy issues and challenges you will need to navigate:



## The Regulatory Landscape

The regulatory landscape is dynamic (see the sidebar for examples). New laws and regulations have emerged to cover more regions, and even established laws like Europe's General Data Protection Regulation (GDPR) undergo revisions. Businesses need to navigate this complexity and ensure compliance with ever-changing requirements.

<sup>1</sup> <https://artificialintelligenceact.eu/the-act/>

<sup>2</sup> <https://time.com/6342551/23andme-hack-health-data-profiles-compromised/>

<sup>3</sup> <https://www.cnn.com/2024/07/12/business/att-customers-massive-breach>



## Governing Data's Infrastructure

Modern data privacy extends beyond personal data to govern the infrastructure through which it flows. New laws like the EU AI Act<sup>1</sup> address entire ecosystems with infrastructure-level requirements for cross-border data transfers, data localization and technology architecture. This will impact how organizations approach cloud adoption, system design and API management.



## Cybercrime and Data Breaches

As recent events involving 23andMe,<sup>2</sup> AT&T<sup>3</sup> and other prominent brands show, the threat of cyberattacks and the risk of data breaches will remain significant concerns. Expect stricter data security regulations, increased focus on incident reporting and response, and ongoing efforts to combat cybercrime.



## Data Sovereignty and Localization

Data sovereignty is the regulatory concept that data is subject to the laws in the country where it is collected or stored. Cross-border data flows face scrutiny that has implications for international business and data-driven innovation. Operational constraints and restrictions on data transfers impact agility, and localizing data can prove costly.



# Data Privacy's Major Landmarks (Continued)



## Data Minimization

Data minimization is the principle of collecting, processing and storing only the personal data essential to achieve a specific purpose. It is incorporated in many data privacy laws globally as a method to reduce exposure to breaches and protect individuals' privacy. While it requires the right tools to implement at scale, minimizing data in systems can also benefit operational efficiency.



## Privacy-Enhancing Computation

Privacy-Enhancing Computation (PEC) techniques like secure multi-party computation and federated learning pave the way for collaborative AI projects that are sensitive to data privacy concerns. PEC algorithms allow the use of AI and machine learning for calculations and insights without revealing raw data.



## AI Ethics and Transparency

Concerns about transparency, bias and potential misuse have intensified as AI applications become ubiquitous. The first tentative steps towards frameworks and regulations — **the EU AI Act**, for example — focus on explainability, mitigating bias in algorithms and embedding ethical considerations in AI initiatives.



## The Power of Trust

Ultimately, building trust is the key to unlocking the full potential of data and AI in a privacy-conscious world. Companies that prioritize transparency, agency and responsible data management practices will stand out as innovators worthy of customers' trust and loyalty.

# Tracking Data Privacy Laws

The complex landscape of data privacy laws has come about through regional efforts to address the global trend towards stronger data protection and privacy rights, driven by the increasing importance of personal data in our rapidly digitalizing world

This selection of regulations exemplifies the similarities and points of divergence in data privacy laws internationally:



## General Data Protection Regulation (GDPR)

Enacted by the European Union in 2018, GDPR is one of the most comprehensive data protection laws. It applies to any organization processing the personal data of EU residents, regardless of location. GDPR emphasizes data subject rights, including consent, access, rectification, erasure and portability of personal data. It also imposes significant fines for non-compliance.

<sup>4</sup> <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>

<sup>5</sup> <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>

<sup>6</sup> <https://www.oag.ca.gov/privacy/ccpa>

<sup>7</sup> <https://www.consumerprivacyact.com/california-privacy-act-2020-cpra/>



## California Consumer Privacy Act (CCPA)

Effective from January 2020, the CCPA<sup>6</sup> provides California residents with rights regarding their personal information held by businesses, regardless of location. It allows consumers to know what data is collected, opt out of data selling and request deletion of personal information. Businesses regardless of location. It allows consumers to know what data is collected, opt out of data selling and request deletion of personal information. Businesses must disclose data practices and are subject to penalties for violations.

The California Privacy Rights Act (CPRA),<sup>7</sup> effective January 2023, builds on the CCPA. It introduces stricter regulations on sensitive information, the right to correct personal data and an enforcement agency. CPRA aligns more closely with global privacy standards, ensuring robust consumer data protection and increasing business responsibilities in handling personal data.



## Personal Information Protection and Electronic Documents Act (PIPEDA)

Canada's PIPEDA<sup>8</sup> regulates the collection, use and disclosure of personal information in commercial activities. It grants individuals rights to access and correct their information and mandates that businesses comply with ten privacy principles, like accountability and limits on data collection. Amendments continue to align PIPEDA with evolving global standards.

# Tracking Data Privacy Laws (Continued)



## **Lei Geral de Proteção de Dados General Data Protection Law (LGPD)**

Translated to English as “General Data Protection Law,” the LGPD<sup>9</sup> governs the use of personal data in Brazil. Inspired by GDPR and effective since 2020, it delivers a broad range of data subject rights and imposes constraints on data processing activities. Companies must designate a Data Protection Officer and comply with strict data protection standards.



## **Health Insurance Portability and Accountability Act (HIPAA)**

In the United States, the late 1990s saw the enactment of pivotal privacy legislation such as HIPAA<sup>4</sup> and the Children’s Online Privacy Protection Act (COPPA),<sup>5</sup> which set standards for the protection of health and children’s data, respectively.

<sup>8</sup> <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/>

<sup>9</sup> <https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/>



# Navigating to Data Privacy Maturity

## The data privacy landscape presents both challenges and opportunities.

Businesses need to adapt to new regulations, embrace privacy-enhancing technologies and build trust with customers, partners and investors through transparency and responsible data practices. Successful organizations will innovate solutions that set themselves apart.

Navigating the complex landscape of data privacy laws involves understanding the impact of regulations on your business and implementing a robust compliance strategy. Compliance efforts today will help your organization reach a sustainable future where responsible data practices benefit everyone.

For organizations with established programs to govern and address the myriad privacy laws around the world, the next evolution requires intelligence automation, deep integration with technology governance, and privacy-enhancing capabilities embedded throughout the data lifecycle.

Here are six checkpoints to help you plot a course:



### Chart Your Landscape

Map your operations to understand which laws and industry-specific regulations apply to your organization. The General Data Protection Regulation (GDPR), the Lei Geral de Proteção de Dados (LGPD), the

Personal Information Protection and Electronic Documents Act (PIPEDA), the California Privacy Rights Act (CPRA) and more — every data privacy law has different requirements.. Dive deeply into key provisions to understand how required security measures (including cross-border data transfers) and data subject rights, such as consent, retention and deletion, impact your business practices.



### Enhance Data Security

Invest in robust data privacy and security capabilities that allow you to implement automated access controls and data protections across all your data stores and systems, with regular security audits. At the same time, educate your staff on data security best practices and train them on secure data handling and incident response procedures.



### Embrace Transparency

Be transparent about your use of data and AI. Explain how algorithms are used and what you do to mitigate risks and potential biases. You could offer choices to opt out or restrict AI data collection and processing to give data subjects some influence over AI-generated data.



# Navigating to Data Privacy Maturity (Continued)



## Build a Data Privacy Culture

Integrate privacy considerations in every stage of product development and business operations. Map the flow of personal data through your systems to embed privacy by design. Meanwhile, update your privacy policies to be concise, accessible and explain your data practices clearly for users and customers.



## Support Awareness and Education

Provide employees with the knowledge and tools to stay compliant as data privacy challenges become increasingly complex. Create initiatives to raise user awareness, promote data privacy as part of data literacy and train individuals in the skills to navigate data privacy laws with confidence.



## Prepare to Adapt

Stay informed about evolving laws and change your compliance strategy accordingly. Ensure someone in your organization is responsible for monitoring regulatory updates and do not be shy to seek expert guidance from legal or data privacy professionals whenever you need specific advice.



# Questions About the Future

## The future promises more dramatic changes.

Business leaders should explore potential scenarios that could shape data and AI operations before their competitors realize what hit them.

Here are six questions to help you consider directions you might have to take in the future:

### Will surveillance and government access increase?

With growing concerns about online safety, disinformation and cybersecurity, some governments have already pushed for increased surveillance powers and access to devices and data. While laws seek to strike a balance between public safety and privacy, businesses in the future may face new requirements to account for data in their systems.

### Will data subjects get more control?

The debate about how individuals can benefit from the value their data generates is likely to continue. Some individuals will regain control over their information, storing it on personal data vaults or trusted decentralized platforms. If such a shift were reflected in new regulations, businesses would need innovative solutions to support personal data portability, user-controlled data monetization and secure data sharing.

### Will we have to explain AI-driven decisions?

Imagine if we all understood how our newsfeeds prioritize posts or why our credit applications are settled one way or another. Consumer expectations could establish explainable AI as a cornerstone of future AI legislation. Explainability, revealing algorithms and decision-making processes, has the potential to build trust and encourage fairness, but adds complexity for organizations that manage AI-driven systems.

### Will AI governance and privacy converge?

As AI laws and regulations mature alongside existing and evolving privacy frameworks, organizations face the challenge of unifying these governance streams. Privacy teams must collaborate with AI ethics committees to implement automated impact assessments, bias detection, and explainability requirements. The organizations that succeed will leverage unified platforms that can manage both privacy policies and AI governance controls across their data estate.

### Will AI be useful for data privacy?

Data privacy and AI won't just be seen as a clash of titans. Expect exciting developments in AI-powered solutions that enhance privacy, like intelligent anonymization tools for sensitive data analysis use cases or fraud detection systems that dynamically protect identities.

# Questions About the Future (Continued)

## Will there ever be regulatory harmony?

While regional regulations already influence each other and set minimum standards for data privacy and security, a global regulatory framework for data privacy is not on the table. Some level of convergence could emerge, but diverging laws would mean more complexity for businesses to deal with. Every different data privacy law has a ripple effect that affects businesses to greater or lesser degrees.





# How Technology Helps

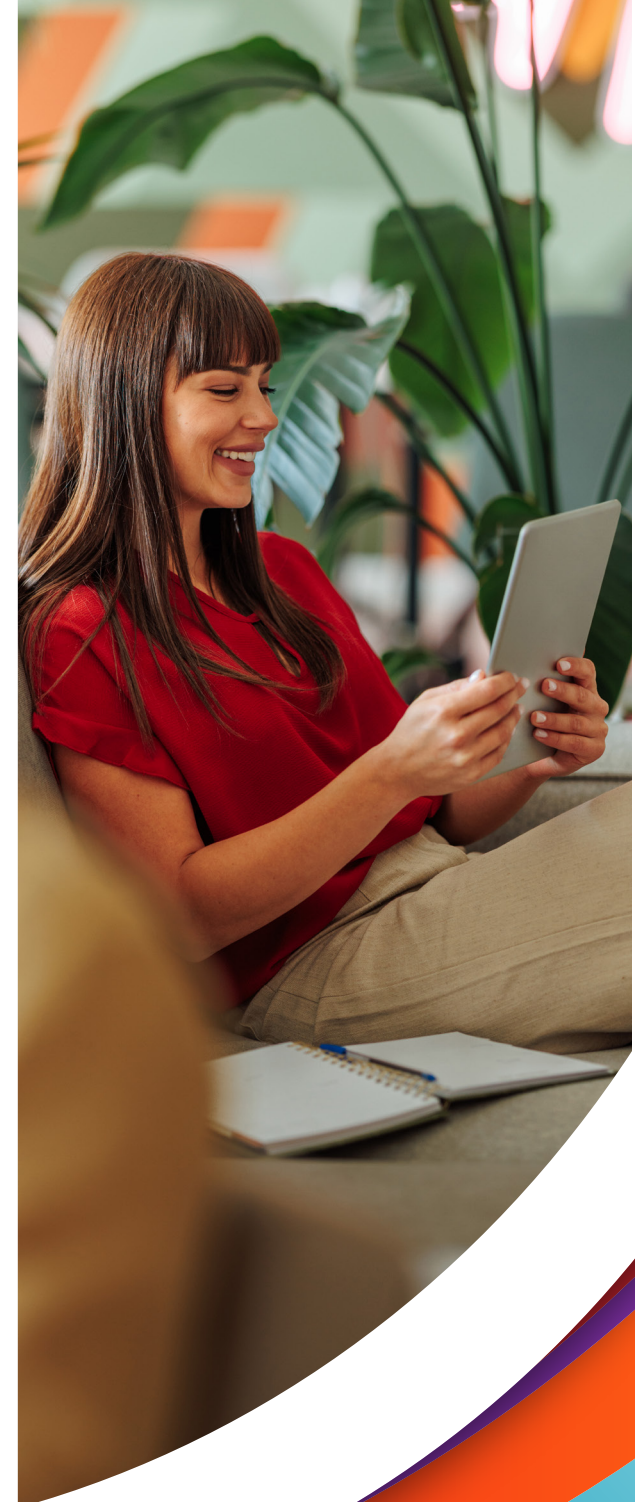
**Data privacy presents opportunities to build trust with customers and gain a competitive advantage when your organization is perceived as a leader in responsible data management and AI practices.**

Equip your organization with robust, automated and intelligent data governance capabilities to seize these opportunities.

**The Informatica Intelligent Data Management Cloud™ (IDMC)** delivers comprehensive, AI-powered capabilities that help minimize risk and maximize transparency to support compliance throughout the data lifecycle.

Automated data discovery, classification, policy execution and monitoring facilitate safer data use and help to avoid regulatory penalties. IDMC's cloud-native services offer the flexibility and scalability to adapt to new and evolving regulatory mandates.

Data integration, mastering and quality controls, data protection, access controls and a secure data-sharing marketplace work together to ensure clean, accurate, transparent and consistent data is ready for compliance reporting whenever needed, all with a single platform.





# About Us

Informatica (NYSE: INFA), a leader in enterprise AI-powered cloud data management, brings data and AI to life by empowering businesses to realize the transformative power of their most critical assets. We have created a new category of software, the Informatica Intelligent Data Management Cloud™ (IDMC), powered by AI and an end-to-end data management platform that connects, manages and unifies data across virtually any multi-cloud, hybrid system, democratizing data and enabling enterprises to modernize their business strategies. Customers in approximately 100 countries and more than 80 of the Fortune 100 rely on Informatica to drive data-led digital transformation.

**Informatica. Where data and AI come to life.™**

IN19-5168-0625

© Copyright Informatica LLC 2025. Informatica and the Informatica logo are trademarks or registered trademarks of Informatica LLC in the United States and other countries. A current list of Informatica trademarks is available on the web at <https://www.informatica.com/trademarks.html>. Other company and product names may be trade names or trademarks of their respective owners. The information in this documentation is subject to change without notice and provided "AS IS" without warranty of any kind, express or implied.

[informatica.com](https://www.informatica.com)

**Where data & AI come to**



Worldwide Headquarters  
2100 Seaport Blvd.  
Redwood City, CA 94063, USA  
Phone: 650.385.5000  
Fax: 650.385.5500  
Toll-free in the US: 1.800.653.3871

[informatica.com](https://www.informatica.com)  
[linkedin.com/company/informatica](https://www.linkedin.com/company/informatica)  
[x.com/Informatica](https://www.x.com/Informatica)

**CONTACT US**