Amplitude

# Guide to Global Customer Data Privacy

# Table of contents

# Data compliance is complex

Navigating today's privacy and security landscape is anything but straightforward, presenting a complex and ever-evolving challenge. The business world's growing reliance on data and technology has elevated the importance of safeguarding consumer information. High-profile incidents have underlined the urgency of this task.

Take, for instance, the case of Cambridge Analytica, which exploited personal data from millions of Meta users for political purposes, sparking global outrage.[1] Then there's Meta itself, grappling with ongoing privacy concerns and security breaches.[2] Google has also faced its share of controversies, from data breaches to GDPR compliance, emphasizing the need for robust data protection.[3] Even ByteDance, the parent company of TikTok, has not been immune to scrutiny, particularly regarding the handling of user data, especially among younger audiences.[4]

Privacy and security are not abstract notions. Data compliance is tangible, with direct consequences. But, it's also extremely complex and challenging. In this guide, we'll delve into the heart of these challenges, offering practical insights and best practices to help you safeguard your customers' data and better understand compliance with international privacy laws and regulations.

## The pressures for getting data compliance right are mounting

Digital transformation and the widespread adoption of cloud technologies enable organizations to expand their horizons and engage in borderless business. However, this global growth brings new security vulnerabilities and risks.

In fact, a staggering 67% of businesses[5] are struggling with cloud adoption, which can expose them to data security vulnerabilities. This struggle highlights the need for businesses to adapt and strengthen their data security measures in the face of evolving technology landscapes.

Approximately 70% of businesses report generating at least 25% more data each year.

Moreover, companies are now using and storing more data than ever, and implementing new systems and technologies can often lead to blind spots in security. Approximately 70% of businesses report generating at least 25% more data each year.[6] This data explosion presents both opportunities and challenges.

To add to this complexity—companies use, on average, 16 different technology applications to manage customer data and rely on 25 different sources for generating customer insights and engagements.[7] These multipart ecosystems underscore the growing importance of safeguarding customer data in an era of rapid digital expansion.

## The expanding landscape of global data privacy compliance

Navigating the complex terrain of global data privacy compliance is an ongoing challenge for businesses. Europe, in particular, has been ahead of the curve regarding data privacy legislation, with regulations like GDPR setting the consumer protection standard. However, significant challenges exist on both sides of the Atlantic.

A remarkable 71% of countries now have data privacy legislation in place, and many are continually refining their privacy regulations.[8] This evolving

global regulatory environment adds layers of complexity for organizations striving to maintain compliance and safeguard customer data.

What makes this challenge even more daunting is the fact that only 34% of organizations have conducted comprehensive data mapping and truly understand data practices across their organization.[9] This lack of visibility can leave businesses vulnerable to compliance gaps and data security risks.

In addition, IT leaders face substantial data security and governance challenges—a staggering 90% report grappling with significant challenges in this regard.[10] These problems underscore the critical importance of staying abreast of global data privacy compliance requirements, as well as the need to implement robust data security and governance measures.

## The shift from third- to first-party data: opportunities and challenges

A significant paradigm shift is underway as companies transition from relying on third-party data to adopting first-party-centric approaches. This shift gives organizations complete control over how and why they collect data, offering numerous benefits such as personalized marketing activities and improved accuracy in targeting audiences.

However, this transition also brings forth a set of privacy challenges—placing the responsibility for data security squarely on the shoulders of the individual company.

Embracing first-party data can increase consumer trust as customers are increasingly willing to share their data for the sake of personalization, recognizing the value it can bring to their online experiences. Building trust through transparency and responsible data management is a crucial part of this transition.

What's propelling this shift toward first-party data approaches is not only the pursuit of more accurate and personalized marketing but also a response to global data protection efforts and legislation. As countries around the world tighten their data privacy regulations, it's becoming essential for businesses to adopt practices that respect customer privacy and ensure the security of the data they collect.

# What's happening today and why it's falling short

Organizations continue to adopt additional systems such as databases, data warehouses, and data lakes, which lead to more data silos. Many of them are unable to keep up with this growing volume and variety of data.

Organizations lack visibility across their data. Without visibility, it's challenging to apply the right policies and controls across their data. Eventually, a user will gain access to data they shouldn't.

Data privacy rules and regulations are complex and will continue to change and proliferate. Yet organizations are struggling to keep up with the right level of training, which breeds risk for compliance issues.

At the perceived expense of proper security and compliance practices, some organizations may try to get by with legacy processes. Often the consequences are much greater than the cost of prevention with a robust governance approach.

## Noncompliance is costly

Noncompliance with data privacy regulations can exact a hefty toll on businesses, often proving more expensive in the long run than investing in compliance measures. The costs of noncompliance encompass various dimensions:

- **Fines:** In the EU, companies can face fines of up to 4% of their global annual revenue for violating the General Data Protection Regulation (GDPR).[11] These fines can be substantial, leading to financial strain and legal complications.
- **Loss of customers**: 71% of customers would consider leaving a company if it shared their sensitive data without their permission.[12] This highlights the significant impact that breaches of trust can have on customer loyalty and retention.
- **Business disruption and productivity loss:** Noncompliance often triggers resource-intensive legal proceedings and damage control efforts, disrupting day-to-day operations and hindering productivity.
- **Revenue loss and stock value decreases:** A significant 41% of executives pointed to revenue loss as the primary consequence of noncompliance.[13] Furthermore, stock price reactions to negative press are 9x larger than the actual penalties incurred.[14] This underscores the profound impact that noncompliance and data breaches can have on a company's financial performance and market standing.

# Better understand international privacy laws and regulations

Regulations that impact data protection vary by country — or within the US, by region, state, and sector—and they are consistently evolving and changing. To navigate this complex landscape effectively, we help break down the most significant and impactful data protection regulations shaping and influencing the regulatory landscape. These regulations can have substantial implications for your business.

In the following sections, we will delve into the key aspects of GDPR and other major global data protection regulations, helping you understand their implications and the steps you need to take to ensure compliance.

## The gold-standard data protection regulation: GDPR

The General Data Protection Regulation (GDPR) is an EU-based data privacy law that sets rigorous guidelines to protect the individual privacy rights of EU residents. It imposes significant restrictions on how companies can gather, process, and use customer data.

GDPR has become synonymous with data protection excellence, and its impact extends beyond the borders of the European Union. Even if your company is not based in the EU, if you collect and process data from EU residents, you are subject to GDPR's requirements. The regulation's reach is global, making it a paramount consideration for any business that handles customer data.

### Understanding GDPR principles

The GDPR operates on 7 key principles:

1. **Lawfulness, fairness, and transparency**
    - **Lawfulness -** You have a legal basis for using the personal data (e.g. gaining consent for use).
    - **Fairness -** Your processing of the data is in the best interest of the person.
    - **Transparency -** You've communicated what, how, and why the data you are processing is used.
2. **Purpose limitation -** Data is only processed in the way you originally intended and it won't be reused for other purposes.

3. **Data minimization -** You're gathering only the data necessary to deliver.
4. **Accuracy -** You have updated or deleted any inaccurate data.
5. **Storage limitations -** Similar to purpose limitation, you shouldn't keep data you no longer need or that isn't of use for the original purpose for which it was intended.
6. **Integrity and confidentiality -** Personal data is correct, being used safely, and only the people who need to access it have access.
7. **Accountability -** The processor is accountable for processing personal data in compliance with GDPR.

## Amplitude's GDPR compliance

Amplitude aligns with GDPR principles and requirements to ensure data privacy and protection. For detailed information on our GDPR compliance, explore our compliance resources.

Learn more about Amplitude's GDPR Compliance

## GDPR 3 key privacy and security requirements explained

### 1. GDPR data residency

Under GDPR, companies that handle personal data of EU citizens must ensure adequate data protection. This can be achieved by either storing and processing that data within the EU or other countries with equivalent data protection measures in place or by implementing other measures to ensure data is adequately protected when transferred outside the EU.

### 2. GDPR the right to be forgotten

Privacy regulations give end users control over their personal data by enabling them to request that their data be deleted.

### 3. GDPR data subject access requests

End users have the right to access their personal data that is being processed by an organization, including how this data is being used, who it is being shared with, and how long it will be retained. Organizations are required to respond to these requests within 30 days of GDPR and provide the data in an easily understandable format.

# US data privacy and protection laws

In the United States, data privacy is a complex patchwork of federal, state, and sector-specific laws, with no national standard governing data protection. A growing number of states have taken it upon themselves to pass data privacy legislation, reflecting the increasing significance of this issue. As of the end of 2023, 12 states have passed data privacy legislation, four are active now, and a number of other states have introduced and are considering similar measures.[15] These state-specific laws add layers of complexity for businesses that operate across state lines or interact with consumers nationwide.

## Examples of state data privacy laws:

1. California Consumer Privacy Rights Act (CCPA): Often considered the strictest U.S. data privacy law, CPRA applies to businesses collecting personal information. It grants Californians the right to know what data is collected about them and enables them to object to data sales. Ensuring CPRA compliance is crucial for businesses interacting with Californian consumers.
2. Colorado Privacy Act (CPA): CPA provides Colorado consumers with rights to access, delete, and correct personal data and opt out of data sales and targeted advertising. It also imposes obligations on businesses to protect data, provide transparent data practices, conduct assessments, and obtain consent for sensitive data processing.

In addition to state laws, certain industry-specific regulations like the following examples also play a crucial role in data privacy:

1. Health Insurance Portability and Accountability Act (HIPAA): HIPAA safeguards health information privacy and security, ensuring patients' rights to their health data. Compliance is vital for healthcare entities, including providers, insurers, and business associates.
2. Special Protections for Children: The Children's Online Privacy Protection Act (COPPA) The Children's Online Privacy Protection Act (COPPA) protects online privacy for children under 13. It imposes strict requirements on websites and online services collecting data from children, fostering a safe online environment.

### How Amplitude adheres to and enables our customers' compliance with HIPAA

- **Data Control:** We provide tools for data control, aligning with CCPA and HIPAA.
- **API Support:** Our platform includes APIs for end-user data requests.
- **DPAs:** We offer DPAs with EU Standard Contractual Clauses for data transfer.
- **SDK Flexibility:** You control data collection and storage.
- **Advanced Features:** We enable individual information removal and IP address control.

Learn more about Amplitude's compliance

# Additional global legislation

As the importance of data privacy continues to grow, governments worldwide are taking measures to implement modern privacy regulations to protect their citizens' personal information. It is estimated that by the end of 2023, approximately 75% of the world's population will have its personal data covered under such regulations.[16] This signifies a global recognition of the fundamental importance of safeguarding individual privacy.

It's important to note that while a significant portion of the world has implemented privacy legislation, the landscape remains diverse. Seventy-one percent of countries have enacted data privacy legislation, while 9% are in the process of drafting legislation, and 15% have yet to establish any data regulations at all.[17] This variation in the global data privacy landscape highlights the need for businesses to remain vigilant and adaptable in navigating these diverse regulatory environments.

Here are some examples of country-based legislation that play a pivotal role in shaping the global data privacy landscape:

- Canada's Consumer Privacy Protection Act (CPPA) - Canada
- The Privacy Act 1988 - Australia
- Brazilian General Data Protection Law (LGPD) - Brazil
- Singapore's Personal Data Protection Act (PDPA) - Singapore
- The Digital Personal Data Protection Act, 2023 - India

Each of these regulations places distinct requirements and obligations on businesses operating within their respective jurisdictions. Understanding these global data privacy laws and their implications is essential, especially if your organization conducts international operations or serves customers across borders.

## How Amplitude adheres to global privacy

### Amplitude's Data Processing Addendum (DPA)

A globally applicable legal agreement that establishes the legal framework under which Amplitude processes personal data submitted to the Amplitude services by a customer and applies to all of our services in accordance with global privacy laws.

Learn more

# New technologies and emerging compliance requirements

As technology evolves, it brings forth new capabilities and challenges for data privacy, leading to the proposal of additional regulations. The growing use of geolocation, biometric data, and artificial intelligence (AI) is prompting governments to consider and craft legislation to address these emerging concerns.

For instance:

- AI Ethics Framework Proposal (AI Act) - European Commission: Proposed in 2021, the AI Act is set to become the world's first comprehensive legal framework for artificial intelligence. This framework aims to establish clear ethical and operational guidelines for AI applications, emphasizing transparency and accountability in the development and use of AI technologies.
- National AI Commission Act - US: This proposed bill introduces a risk-based framework for regulating artificial intelligence within the United States. As AI continues to transform various sectors, including healthcare, finance, and transportation, this bill seeks to ensure that AI is developed and used in a manner that mitigates potential risks and safeguards privacy.

The rapid advancement of technologies like AI presents novel privacy challenges that require forward-thinking legislation. Understanding and preparing for these evolving compliance requirements is essential for businesses that leverage cutting-edge technologies.

# Common themes in global legislation: What to know and prepare

Given the complex regulatory landscape, it can be challenging to identify a single, universally applicable data protection framework. However, amidst the diversity of global legislation and consumer data protection laws, there are common themes that every organization should understand and implement to ensure compliance and protect customer personal data (CPD).

## Understanding your use of customer personal data (CPD)

A fundamental step in data protection is understanding the scope and nature of the **customer personal data (CPD)** that your organization handles. The definition of personal data or personally identifying information (PII) varies between different regulations but is a critical concept. It generally includes any data that can be used to identify an individual, whether directly or indirectly.

Examples of PII include names, phone numbers, addresses, IP addresses, device IDs, and email addresses. It's essential to recognize that the definition of what qualifies as PII has evolved over time, particularly with the implementation of CCPA, and can vary by region. Staying current with these definitions and identifying PII within your data is crucial.

## Sensitive personal data

Many data protection regulations require heightened protection for sensitive personal data (or sensitive PII) due to its potential for misuse. Sensitive personal data typically includes details such as credit card numbers, social security numbers (SSNs), financial information, health information, genetic data, and biometric information. The inclusion of this category in data protection laws underscores the importance of safeguarding data that, if mishandled, could have serious consequences for individuals.

## Additional responsibilities to protect the personal data of minors

Protecting the personal data of minors is a shared concern across various data privacy regulations. These laws often impose additional responsibilities on organizations when handling the personal data of individuals under a certain age, typically individuals under 13 or 16, depending on the jurisdiction. Ensuring the compliant handling of minor's data is a critical aspect of maintaining data privacy and regulatory adherence.

## Minimize your use of personal data to just what's needed

A key principle in data privacy is data minimization, or minimizing the use of personal data to only what's necessary for the intended and disclosed purpose. This principle is fundamental to many data protection regulations.

Obtaining valid consent for collecting and processing personal data is a core requirement under many data privacy regulations. Consent must be freely given, specific, informed, and unambiguous. In order to obtain freely given consent, it must be given on a voluntary basis. Accordingly, businesses should provide a clear definition of what data is collected, for what purpose, how it is used and protected, and with whom it may be shared. Websites and online services must allow users to opt out of tracking and data collection, providing them with choices regarding certain data processing, sales of their data, and the processing of sensitive information.

## Consider data sovereignty and residency

Digital data is subject to the laws of the country where it is located. This concept is known as data sovereignty. Additionally, some countries have introduced legislation that requires the personal data collected to be stored within specific geographic locations or to ensure that appropriate safeguards and/or adequate protection for that data can be met. This requirement is aimed at protecting the privacy and security of individuals' personal data.

## Other consumer rights that matter

Several consumer rights are integral to data protection regulations, including:

- **Right to access, correct, and delete:** Individuals have the right to access the personal data that organizations hold about them, correct inaccuracies, and request the deletion of their data.
- **Right against automated decision-making:** Regulations often include safeguards against purely automated decision-making processes that could significantly impact individuals.
- **Private right of action:** This provision allows individuals to take legal action against organizations that violate data protection laws, further empowering individuals to protect their rights.
- **Right to opt-out of data sale and sharing:** Individuals can opt out of having their personal data sold or shared by organizations, providing further control over their data.

## Obligations for businesses

To ensure compliance with data protection laws, businesses are often obligated to:

- Provide clear and transparent notices to users, explaining how their data is collected, processed, used, and shared and how they may exercise their data rights.
- Ensure valid consent for data processing, especially when involving minors, keeping in mind that consent requirements may vary by country (e.g., EU's default opt-out vs. US's opt-out option).
- Conduct risk assessments to identify and mitigate data privacy risks within their operations.
- Prohibit discrimination against individuals exercising their data privacy rights.
- Adhere to purpose and processing limitations, ensuring that data is only used for the specific purposes for which it was collected.

# Privacy and security framework: strategies and best practices

Navigating the complexities of global data privacy regulations and ensuring robust data protection requires a comprehensive framework and strategic approach. Let's outline some best practices to help your organization establish an effective privacy and security framework, reducing risks and safeguarding customer data while ensuring compliance with global regulations.

## Use a multi-stakeholder approach

Data security and privacy initiatives must begin with strong executive support and involve collaboration from cross-functional teams. Define and assign roles and responsibilities within your organization. Consider appointing a Data Protection Officer (DPO) or Privacy Officer to oversee data protection efforts.

## Implement data governance

Develop and maintain a robust data governance strategy that includes regular reviews and updates. Keep track of the data you collect and ensure that it's managed according to your defined policies and standards. For additional context, refer to Amplitude's blog post on data governance.

## Conduct a comprehensive data inventory

Perform an inventory of all structured and unstructured data within your organization to identify potential gaps and challenges in data protection. This step is crucial for understanding what data you collect, where it's stored, and who has access to it.

## Protect consumer data privacy

Map your data repositories, access and permissions, and data processing processes to ensure that you can identify and secure important data. Be prepared to access, delete, and transfer personal data as required by data privacy regulations.

Amplitude offers a User Privacy API that helps you comply with end-user data deletion requests.

## Implement a transparency-focused privacy policy

Transparency is not only a legal requirement in many countries but also an expectation of customers. In fact, 86% of consumers want transparency regarding the use of their personal information.[18] Clearly communicate to consumers how you collect, process, and use their data and make it easy for them to locate your policy and submit a data request.

## Centralize data management

Replace legacy on-premises systems with modern digital analytics solutions that enable efficient responses to customer requests for access, correction, or deletion of data. Ensure that the solution integrates seamlessly with your existing technologies and enables you to control data flows while providing guidance and clarity on the privacy landscape.

## Implement appropriate access controls

Understand and manage who within and outside your organization has access to sensitive data. Implement user authentication, identity access management, and data access roles and permissions to control and monitor data access effectively. Consider a product-led privacy approach to customer data.

86% of consumers want transparency regarding the use of their personal information.[18]

## Use data encryption

Data encryption serves as a fundamental safeguard for sensitive information, offering protection both when data is stored (at rest) and when it's transmitted (in transit). By employing advanced encryption techniques, organizations can ensure that their data remains secure and impervious to unauthorized access.

## Implement data loss protection and data recovery

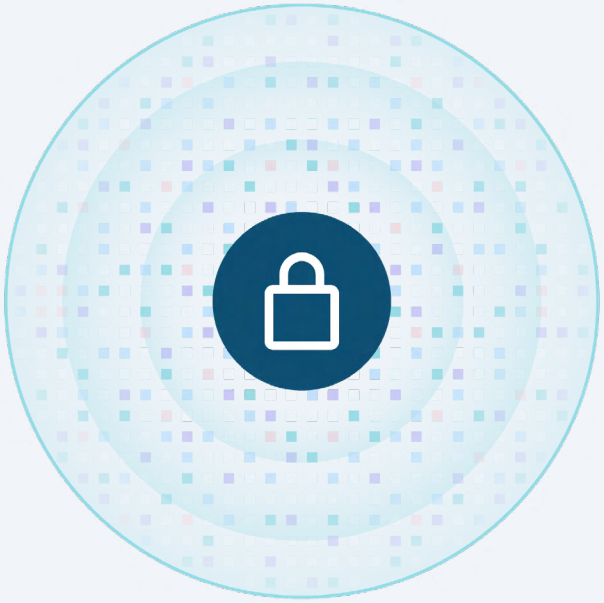
Preventing data breaches and unauthorized access and the ability to recover data quickly is paramount. In addition to data encryption, organizations should consider implementing Data Loss Prevention (DLP) solutions, anti-ransomware, and resiliency controls to help achieve this. This will help provide a proactive defense against data loss incidents, helping organizations identify, monitor, and protect against potential threats. With data loss protection and data recovery measures in place, organizations can minimize risks and maintain the integrity of their data assets.

# Building trust through comprehensive data protection

While these best practices are essential components of a robust privacy and security framework, they are not the sole determinants of maintaining compliance or preventing data breaches. Instead, they form the foundation upon which your organization can better protect customer data and work toward compliance with global data privacy regulations.

By diligently following these best practices, your organization can significantly reduce the risk of costly data breaches and legal repercussions. However, it's essential to recognize that data privacy and security are ongoing endeavors that require continuous effort and vigilance. These steps, when implemented effectively, contribute to building trust with your customers by demonstrating your unwavering commitment to their privacy and data security.

# Help safeguard your privacy and compliance with Amplitude



Data privacy and security can feel overwhelming—but it doesn't have to. Amplitude is your trusted partner committed to helping you safeguard your privacy and compliance. We take a privacy-first approach in every aspect of our product development, ensuring that our customers can confidently use our products in a way that enables their compliance with navigating the complexities of global privacy laws and regulations.

## Amplitude's privacy principles:

- **Your privacy and the privacy of your users' data are our priorities.** We place the utmost importance on safeguarding your data and ensuring the privacy of your users. Our commitment is unwavering, and we continuously innovate to protect your information.
- **Our goal is to make it easy for you to be compliant.** We provide you with the tools, features, and guidance you need to effortlessly maintain compliance with the latest privacy laws and regulations, reducing the complexities and risks associated with data management.

**Curious about our credentials? Amplitude is SOC 2 Type 2 and ISO 27001 and 27018 certified, underscoring our commitment to data security and privacy.**

- **We provide you with the tools to be in control of your data.** We empower you to take control of your data, allowing you to manage, access, and protect it in line with your business needs and legal requirements.
- **We prioritize data protection through technology design.** At Amplitude, we integrate data protection into our technology design, ensuring that your data is secure from the ground up.

## Take the next step in safeguarding your data by learning more about how Amplitude can support your privacy and compliance efforts.

Learn more

## Endnotes


1. The New York Times: "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far" (2018)
2. The Guardian: "Meta fined €265m over data protection breach that hit more than 500m users" (2022)
3. Wired: "Europe's Move Against Google Analytics Is Just the Beginning" (2022)
4. Buzzfeed.News: "Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China" (2022)
5. Frost & Sullivan: "The Data Protection Guide For Enterprise Modernization" (2022)
6. ibid.
7. Deloitte Digital: "How to win on customer experience" (2023)
8. UNCTAD: "Data Protection and Privacy Legislation Worldwide" (2023)
9. Womble Bond Dickinson: "2023 Global Data Privacy Law Survey Report" (2023)
10. Salesforce: "Global Data Security Trends 2023" (2023)
11. Gartner: "5 Ways to Show Prospects You Take Data Privacy Seriously" (2022)
12. McKinsey & Co.: "The consumer-data opportunity and the privacy imperative" (2020)
13. Deloitte: "Global Survey on Reputation Risk" (2015)
14. ECGI: "Regulatory Sanctions and Reputational Damage in Financial Markets" (2015)
15. Roll Call: "Data privacy law seen as needed precursor to AI regulation" (2023)
16. Gartner, "The Top 8 Cybersecurity Predictions for 2021-2022" (2021)
17. UNCTAD: "Data Protection and Privacy Legislation Worldwide" (2023)
18. Salesforce, "4th Edition, State of the Connected Customer" (2023)

## About Amplitude

Amplitude is a leading digital analytics platform that helps companies unlock the power of their products. Nearly 2,500 customers, including Atlassian, NBCUniversal, Under Armour, Shopify, and Jersey Mike's, rely on Amplitude to gain self-service visibility into the entire customer journey. Amplitude guides companies every step of the way as they capture data they can trust, uncover clear insights about customer behavior, and take faster action. When teams understand how people are using their products, they can deliver better product experiences that drive growth. Amplitude is the best-in-class analytics solution for product, data, and marketing teams, ranked #1 in multiple categories in G2's 2024 Winter Report. Learn how to optimize your digital products and business at amplitude.com

Amplitude Power to your products™