Your Guide to Customer Trust in a Privacy-Centric World

TEALIUM®

Alex Cash
Director of Strategy, Consent & Preferences | CIPP/E | CIPM
OneTrust

Digital experiences are undergoing an upheaval, and we're all impacted. Whether we're marketers, technologists, compliance professionals, or simply individual consumers; we're all experiencing rapid change in our digital lives, whether we know it or not.

So, what is it that's driving this changing digital landscape? First and foremost, it's the change around customer data privacy happening around the world. I always talk about three primary drivers; each distinct yet intrinsically linked.

The three primary drivers of change are:

1. Browsers and operating system changes
   Chrome, Safari, Firefox, iOS, Android, tvOS to name a few – every digital channel we use to engage with consumers is changing, restricting marketers' ability to track users for targeting, attribution, and more.

2. **Legislative changes**
   Modern privacy laws around the world are affording consumers new rights and controls over who can use their data, for what, and for how long. Noncompliance can be financially and reputationally ruinous.

3. **Evolving consumer expectations**
   Consumers expect control, whether that's the ability to consent, opt out, object, or request data deletion; privacy changes have driven UX changes that individuals have grown used to. Getting these wrong can have irreversible consequences for consumer trust, trust that businesses rely on to succeed.

These drivers have converged to force businesses to evolve. No longer can marketers rely on tracking everyone everywhere all the time with third party cookies and device IDs. No longer can we indiscriminately embed tags and SDKs across our websites and apps. So, how can marketers become privacy practitioners, technologists, and consumer experience professionals to thrive in this new paradigm?

Once we understand our privacy obligations, the biggest area of focus is data.

We need to audit what is being collected on our digital properties, who we're sharing it with, and how we enforce consumer privacy decisions. We need to look at how we build trust to capture more data from the right consumers, and thus enable us to satisfy our tracking, targeting, personalization, and measurement needs in a compliant way. The way to bring this privacy-centric approach to customer experience to life is to combine our data and privacy strategies around a Customer Data Platform (CDP), embedding audit and control throughout, to minimize risk, maximize marketing value, and future proof ourselves to the ongoing changes in the technology landscape.

CHAPTER 1

The New State of Privacy and the Value of Compliance

The evolution of privacy regulations and the handling of customer data has undergone significant transformation in recent years, driven primarily by technological advancements and the growing global concern over data protection in relation to data breaches, unauthorized access, and misuse of personal information.

In today's data-driven world, personal information is constantly collected and shared which has necessitated the need for robust privacy safeguards not only for individuals, but for businesses as well. One may initially perceive these ever-evolving global privacy regulations as a hindrance, but in fact they are a benefit to businesses and the consumers they serve.

Businesses that are compliant with privacy regulations benefit from increased customer loyalty and trust as well as the mitigation of risks associated with data breaches and potential legal liabilities. In addition, adherence to privacy regulations fosters a culture of transparency, accountability, and ethical data practices, enabling businesses to navigate the complex landscape of customer data with confidence and provides them with a competitive advantage.

The biggest challenge companies face is how to future-proof their business, technology, and data strategies to ensure they are and will remain compliant with newly evolving global privacy regulations.

This paper explores the evolving landscape of privacy regulations, financial advantages of compliance, importance of proper data collection, pillars of a modern data foundation, and the importance of a proactive privacy consent and governance strategy. It also examines regional and industry impacts of privacy regulations, identifies the teams and roles required to support compliance, and highlights the role Customer Data Platforms (CDPs) like Tealium can play in enabling organizations to shift the complex privacy landscape into a competitive edge.

01

The Growing Costs of Noncompliance

Governments around the world are cracking down on infractions against customer data privacy regulations. Data breaches or the mishandling of customer data in accordance with regulations like the General Data Protection Regulation (GDPR) or California Privacy Rights Act (CPRA) has resulted in staggering fines imposed by regulatory authorities, reaching into the millions and sometimes billions of dollars. Though compliance is mandatory, there are some major financial benefits to adhering to global privacy laws.

The Financial Benefits of Data Privacy Compliance

It is undeniable that adherence to global data privacy laws presents numerous benefits, however, there are some key financial benefits businesses should understand. While many would agree compliance may require additional short-term investments in resources and infrastructure, the long-term advantages far outweigh the costs for businesses.

Creating Competitive Advantages

Data privacy has become a significant concern for consumers, and they are increasingly opting to do business with companies that prioritize data privacy. Businesses can differentiate themselves from the competition with their adherence to data privacy regulations thereby attracting privacy-conscious customers. This can lead to increased market share, improved customer acquisition rates, and ultimately improve their bottom line.

Mitigating Fines, Penalties, and Litigation

Noncompliance with data privacy laws can result in significant financial penalties imposed by global regulatory agencies. These fines can be substantial for businesses, especially under regulations like GDPR. By adhering to privacy laws, businesses can mitigate these costly penalties and the risk of legal actions.

Increasing Customer Loyalty and Company Growth

Consumers are savvier than ever and prefer doing business with brands they trust. Data breaches and privacy violations can lead to a loss of customer trust and damage to a business' reputation and financial outlook. When companies demonstrate a commitment to protecting their customer's data and complying with local and global privacy laws, they can build trust and customer loyalty ultimately driving company growth.

Reducing the Risk and Costs of Data Breaches

Businesses that proactively safeguard customer data, can reduce the risk of data breaches and the associated costs. The financial repercussions of a data breach can be extremely significant, including expenses for incident response, forensic investigations, customer notifications, legal actions, and potential loss of business – not to mention the damage to the brand.

Expanding into Global Markets

Countries globally have enacted strict data privacy laws and regulations to protect personal data, such as GDPR and CPRA. By adhering to these regulations, businesses can confidently expand into new global markets without the worry of significant fines or penalties while they grow their bottom line in new local economies.

Managing Risks & Rewards = Commercial Performace

RISKS	REWARDS
Heightened threat environment	Robust cybersecurity for business resilience
Unacceptable use and disclosure	Informed consent to validly realise the economic value of data
Breach of directors' duties	Resolving the privacy-profitability paradox
Administration burdens	Data externalities
Erosion of trust and reputation	Boost digital trust to bolster innovation
Exploiting information asymmetry	Trusted market leader
Revenue loss	The CX multiplier effect

A Challenge and an Opportunity

DATA RIGHTS & OBLIGATIONS	COMPETITIVE OPPORTUNITY
Right to erasure	Trust as the competitive differentiator
Right to restriction of processing	Transparency in a consistent value exchange
Right to data portability	Real-time personalization and high-quality products & services
Right to data minimisation	Optimal data governance
Right to data integrity	The data quality obligation
Right to data security	An agile consent management architecture
Right to access	Segmented 360-degree single customer view
Right to fairness, equity & transparency	Upholding commercial morality

How Data Collection is Evolving

Your first party and zero party customer data are your most valuable asset.

Driven by advancements in technology and the increasing interconnectedness of our lives, organizations are now able to collect vast amounts of data from various sources, including social media platforms, online transactions, IoT devices, and more. However, as the amount of data has expanded, so has the need for a more privacy-centric data collection strategy.

Your data collection strategy is the first step toward achieving compliance because it defines the scope and nature of the required data processing activities within your organization. It must clarify your organization's unique data landscape and legal basis for data processing. You can then identify risks and compliance gaps, establish transparency with your customers and employees, and build a strong compliance framework. How you collect your customer data lays the foundation for implementing privacy measures and ensuring that data processing activities adhere to relevant privacy regulations.

Because zero and first party data are obtained with the explicit customer consent you are already closer to being in compliance with privacy regulations. This value exchange - you offering something meaningful enough for your customer to allow access to their data - helps you also build trust with your customers. This trust is essential in an era where privacy concerns are widespread, and customers are becoming increasingly cautious about sharing personal information.

Zero and first party data are also highly valuable assets due to their accuracy, personalization enablement, and the long-term competitive advantages they unlock. By leveraging these data types effectively, your organization can make better informed decisions to enhance customer experiences and stay ahead in today's data-driven marketplace.

Check out the eBook: Customer Data Integrations 101 to see how Tealium's Customer Data Platform supports customer data collection and organization from all data sources.

DATA-DRIVEN ORGANIZATIONS ARE:

23x
MORE LIKELY
to acquire customers

6x
AS LIKELY
to retain customers

19x
AS LIKELY
to be profitable as a result

McKinsey Global Institute

02

Six Pillars of a Modern Data Foundation

Digital corporate strategies exist to drive revenue, optimize operational processes, and deliver ROI to the business. All of these depend on a supporting Data Strategy. Having a unifying and cohesive Data Foundation drives business efficiencies and synchronizes teams and systems. This results in the trust of the information being leveraged to generate value for the enterprise.

The development of a modern data strategy will constantly evolve especially with the introduction of new privacy legislation, technologies, and the changing need for skill sets. Regardless of this dynamic environment, there are six key pillars that form the basis of an ideal Data Strategy.

When designing your data strategy, each of these six strategic pillars must be addressed, and progress made in one pillar will apply synergies across the rest. These six pillars will also help maintain compliance, build trust, and ultimately achieve your growth objectives in a highly competitive, digital world.

SIX PILLARS OF A
Modern Data Foundation

01. Omnichannel Strategy

The omnichannel strategy focuses on the goal of unifying the multiple touchpoints that customers use to engage with your business sources in order to catalog, manage, and leverage the valuable customer data.

Today's most popular omnichannel touch points include mobile devices, apps, browsers, kiosks, IoT devices, data warehouses, Customer Relationship Management (CRM) platforms, Master Data Management (MDM) software, Consent Management Platforms (CMPs), Preferences Centers, and even spreadsheets. That being said, it is important to unify the data from these touchpoints to avoid duplication and risks. Data reconciliation is a key objective in the Omnichannel strategy, and it is crucial to plan and design a data strategy that considers all the interrelated pillars.

KEY TASKS

- ☑ Create an inventory of all data sources
- ☑ Create a blueprint for each source that indicates what data types to expect from each source. This includes Identity, Personal Identifying Information (PII), navigation, transactional, and behavioral data
- ☑ Document the common Identity values across the omnichannel in preparation for the Identity Resolution mechanism that will be put in place
- ☑ Design an Event Data model that structures all omnichannel data parameters into a modern, flexible Event design. Reuse existing Event definition wherever possible to promote scalable reporting and measurement

02. Privacy Compliance Strategy

Privacy regulations have become intertwined with digital marketing strategies, with prominent brands adopting best practices to ensure compliance while gaining additional information or insights. For example, a business can offer consumers a value exchange such as a coupon or access to a loyalty program in exchange for additional consumer data while clearly stating the purpose and benefits of data collection. Brands that invest in this value exchange strategy experience increasing returns as trust grows, fostering superior loyalty and long-term customer value. The importance of privacy has reached critical mass, driven by transformative changes from trusted brands like Apple and Google.

Compliance strategies also involve data governance, protection, and security practices, supported by privacy-enhancing technologies. While legal teams play a major role, the ramifications extend to any business unit that handles customer data. Regional privacy regulations also introduce variations in instrumentation and delivery, making it crucial for multi-regional brands to address this nuance.

Overall, brands should strive for a “lowest common denominator” strategy, investing in transparency, flexibility, and demonstrating the value propositions of privacy regulations. Efficiently responding to consumer rights like access, erasure, and modification shows trust and prioritization of consumer rights. **In today’s marketing environment, this goes beyond simple cookie banners or detailed privacy policies.** Getting privacy right becomes a competitive differentiator for brands in the long run.

KEY TASKS

- ☑ Create and launch the Value Exchange lexicon, focusing on how it looks, brand awareness, and being transparent
- ☑ Include the Value Exchange requirements in automated data collection and Consent Management Platform (like Cookie Banner and Privacy Policy) to detect and enforce them in real-time
- ☑ Categorize the Event Model to include Privacy Preferences, Consent directives, and associated data enrichment processes like profiling and audience building
- ☑ Create automation rules to enforce Privacy Preferences for Profiles and Audiences, including mapping external Digital Marketing and AdTech vendor platforms
- ☑ Ensure compliance with regional data privacy laws by auditing and reporting all consumer consent data from all devices in the Omnichannel. Integrate chosen BI and Analytics tools to produce necessary reports for stakeholders

03. Real-Time Activity

In today's digital environment, the processing of data in real-time through automation is a must-have. Modalities have evolved, requiring data to be managed quickly or the company may be unable to use it or worse, will not remain compliant or respect consumer preferences. For example, conversion data is temporal and only lasts for a limited time, while consent and privacy preferences must be captured and addressed in real-time or the business may find itself out of compliance.

A Data Strategy cannot be complete without real-time capabilities - it is a must. Identity strategies and the associated Omnichannel Strategy co-exist with the usage of real-time techniques. Real-time capabilities unify identity, consent, and all other data subject to the Event Data model to produce an accurate profile of the consumer.

A CDP's first, most impactful role, is to perform identity resolution in real-time upon the devices in the omnichannel. Without the capability to react to data in real-time, organizations will quickly lose ground to more nimble competitors who have invested in this area.

KEY TASKS

- ☑ Create a customer profile model that goes beyond the previously built Event Data model. It will include all federated Identity data points, navigation, transactional, and behavioral attributes
- ☑ Connect the Customer Data Platform (CDP) with data collection technologies to enable real-time personalization and ensure privacy compliance

04. Identity Strategy

Identity Management is perhaps the most popular topic in digital marketing and AdTech today. This is because the acquisition of identity data opens the door to new techniques and valuable use cases. Valid Identity data provides the means for integration throughout any and all of the digital marketing and AdTech platforms today.

Trusted and authorized identity within customer datasets will be the determining factor as to whether a personalized strategy will be possible to deploy. The modern data strategy for any business must incorporate not only their own unified identifiers for customer data, but also expand the scope to external partners that have identified the same consumer.

The identity strategy should complement the larger data strategy by allowing businesses to orchestrate relevant customer data in real-time to any partner and service provider, as well as internal stakeholders. All business units are jointly responsible for producing, managing, and using identity while continuing to enrich the customer dataset for the benefit of the company.

KEY TASKS

- ☑ Develop an Identity Strategy that includes Owned & Operated properties and external partners involved in Digital Marketing and AdTech strategies
- ☑ Create a list of Identity Data values and where they appear across all channels
- ☑ Design the necessary Identity data for each external vendor, ensuring seamless integration using a CDP
- ☑ Encrypt all identity values in compliance with Privacy Regulations and store them securely within the Omnichannel system, rather than waiting until later stages like a Data Warehouse. Prompt encryption is crucial to minimize risks

05. Multichannel Strategy

Multichannel refers to the various channels businesses use for customer engagement and marketing. To gather data from different sources, Multichannel technology leverages a unified approach, either ingesting files or collecting directly from sources using Software Development Kits (SDKs) or device libraries. Designating a single technology for data collection and unification is more efficient than each Multichannel stakeholder doing it individually. This approach ensures consistency, reduces inefficiencies, and minimizes the risk of duplicate or incorrect datasets. A centralized data foundation allows for unified customer profiles and delivers competitive advantages through automation and journey orchestration.

Implementing a Hub-Spoke model for Multichannel improves productivity and eliminates concerns about data collection, governance, consent, real-time updates, and identity. It enables automated data delivery to each business entity based on their specific needs. This approach is cost-effective and essential for modern multichannel marketing.

To approach modern multichannel marketing in any other way (e.g. spreadsheets, time consuming meetings, validation checks on data that take weeks, etc.) will introduce risk through the lack of automation. Manual processes and outdated methods introduce risks and are insufficient for delivering timely marketing messages and personalized engagement. Automation, seamless integrations, and user-friendly interfaces are key to efficient multichannel marketing.

KEY TASKS

- ☑ Ensure that all Multichannel vendors have secure APIs that can be configured from a centrally managed data management system like a CDP
- ☑ Deliver Data-As-A-Service to the Multichannel using a Hub-Spoke approach, connecting customer data from the Omnichannel to a preconfigured environment of partners in the Multichannel through automated data flows
- ☑ Design both Profile-based activations and Audience-based activations in the Multichannel to achieve sophisticated Customer Journey goals. Instant synchronization with a single point of control, preferably a CDP, is essential for effective management

05. Multichannel Strategy

Examples of different channels:

Social platforms, publisher sites, search platforms, email service providers, and more

Recent innovations like streaming and CTV, display out-of-home, and retail media have also become valuable channels

Owned and operated properties are important, especially for personalized experiences based on real-time data

Internal analytics and business intelligence departments are considered stakeholders in the multichannel as they provide insights for planning and measuring marketing effectiveness

06. Measurement and Attribution Strategy

Advanced analytics and attribution models in modern data strategies optimize marketing efforts by measuring the impact of each touchpoint for maximum return on investment. However, new privacy regulations restrict consumer device tracking and measurement techniques, posing challenges.

Apple's Safari browser has introduced additional restrictions, replacing UTM parameters with contextual information that reveals desired outcomes without personally identifiable information. Google is also adopting contextual approaches for marketing segmentation. These changes affect acquisition marketing and scenarios with anonymous or unknown users, emphasizing the importance of a value exchange where brands receive identifiable and useful data.

To overcome the loss of external data, brands need to incorporate real-time conversion APIs into their strategies. These APIs capture data from multiple sources and stream it securely to the cloud. Measurement and attribution rely on timely, precise, and secure data, making a centralized CDP valuable for marketing and the business intelligence department.

Check out Tealium's Suite of Conversions APIs!

KEY TASKS

- ☑ Export customer data, including profiles and audience segments, to accessible data repositories for measurement tools
- ☑ Automate real-time data flows to vendors with compatible APIs for customer attribution data
- ☑ Embrace contextual advertising and measurement to adapt to new restrictions and data loss
- ☑ Incorporate real-time conversion APIs and utilize a centralized CDP to enhance marketing insights and detect when anonymous customers become known, preserving data lineage throughout their journey

The Modern Data Strategy

Why a Data Strategy is important, and what's involved.

First Party Data Foundation

All data modalities in scope (ML & AI, Anonymous/Known, Derived, Contextual, Batch vs Streaming, Time-bound, and more)

Omnichannel

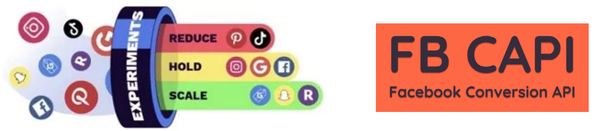
Identity Management

Privacy Regulations & Consent

Multichannel Marketing

Real Time Detection & Processing

Measurement & Attribution



CHAPTER 03

The Proactive Privacy Consent and Governance Strategy & the Role of CDPs

Privacy consent and governance is a dynamic landscape that cannot be set and forgotten, but instead demands a strategic and proactive approach. Global privacy regulations are ever-evolving, and complacency is not an option. Businesses need to drive trust with their customers by developing a privacy consent and governance approach that ensures compliance for all regional and global regulations. They also need to ensure their customers have the ability and power to make informed decisions on how their data is accessed and used.

It is critical to keep in mind that while gathering consent is an essential component of data governance, it is just the starting point. A comprehensive data governance strategy includes a range of measures, such as data quality assurance, security, retention and deletion policies, and accountability, to ensure responsible and ethical data management throughout the lifecycle of your customer's data usage and continued consent - a CDP can help provide the foundation to support these initiatives.

How Customer Data Platforms Support Consent and Governance

The privacy and consent landscape is shifting rapidly and it is critical for brands to be able to quickly adjust in order to provide compelling customer experiences while complying with ever evolving privacy regulations and technology advancements.

Best-in-class CDPs support these business priorities for managing consent as well as enabling organizations to effectively manage and respect customer consent in real-time throughout the data collection and activation lifecycle. A CDP provides agility and scalability, allowing you to adapt to evolving compliance requirements and future privacy advancements without disrupting your data processes.

75%

According to a report by Gartner, by year-end 2024, 75% of the world's population will have its personal data covered under modern privacy regulations.

Why Businesses Need to Future-Proof their Privacy Data Strategies

Expanding global regulations have provided consumers with more control over how their data is collected and managed, which has raised customer privacy awareness and expectations accordingly. Businesses need the ability to control how they collect and utilize data in real-time, ensuring they can activate data quickly (and compliantly), but also ensure there is no misuse of data and they respect consent preferences.

As a key activation point, a CDP is a natural place to govern real-time customer data, giving teams the tools to maintain compliance with expanding global regulations while meeting customer privacy and experience expectations

Regulations globally (combined with technology changes and elevated customer expectations around privacy) restrict data practices, thereby chipping away at a brand's ability to personalize experiences and measure engagement. This is being amplified with third party cookie loss.

A CDP allows businesses to personalize experiences and measure engagement within compliance boundaries, organizing and activating valuable first party data

Gaining explicit consent requires a successful value exchange with customers, being transparent about what is being collected and why so your customers feel empowered to choose what data is being collected and why.

A CDP facilitates a successful value exchange and automates consent management, helping businesses gain explicit consent and build trust with customers while staying compliant

Regional and industry compliance regulations require real-time management of consent data.

A CDP enables real-time consent data management, allowing businesses to capture and update consent preferences promptly

Modern Privacy Governance Framework integrating with other Consent Management Platforms and Preference

THE MODERN DATA GOVERNANCE FRAMEWORK

Privacy Resides at the Intersection of 3 Pillars

TECHNOLOGY	BUSINESS	GOVERNMENT
The tools and capabilities to regulate the flow of personal information and maximise its economic value.	The commercial strategies and strategic decisions that guide the use of personal information to engender profitability in line with market opportunities.	The laws and regulations established by governments and delegated authorities to counterbalance market competition with consumer welfare in a data-driven digital economy.

"Data is a precious thing and will last longer than the systems themselves."

Tim Berners-Lee
inventor of the
World Wide Web

Data Governance
CHECKLIST

01. DATA MAPPING

- ☑ Identify and document the personal data your organization collects, processes, and stores
- ☑ Determine the purpose and legal basis for processing each category of personal data
- ☑ Document data flows, including any data transfers to third parties or outside the organization's jurisdiction

02. LAWFUL BASIS FOR PROCESSING

- ☑ Ensure you have a valid lawful basis for processing personal data (e.g., consent, contract performance, legal obligation, legitimate interests)

03. CONSENT MANAGEMENT

- ☑ Obtain clear and explicit consent from individuals for processing their personal data
- ☑ Provide easily accessible and understandable consent requests
- ☑ Maintain a record of consent and allow individuals to withdraw consent easily

04. RIGHTS OF DATA SUBJECTS

- ☑ Inform individuals of their rights, including the right to access, rectify, erase, restrict processing, and object to processing
- ☑ Establish processes to handle data subject requests within the required timeframes

Data Governance
CHECKLIST

05. CONSENT MANAGEMENT WITH CDPS

- ☑ Implement a Customer Data Platform (CDP) to manage and orchestrate consent on the profile level
- ☑ Ensure that the CDP captures and associates consent preferences with individual profiles
- ☑ Enable real-time synchronization of consent preferences across channels and devices for a consistent user experience
- ☑ Leverage user authentication mechanisms (e.g., login credentials) to recognize and maintain consent preferences across different interactions
- ☑ Minimize the need for repetitive consent requests by intelligently recognizing authenticated users and their consent preferences

06. DATA SECURITY

- ☑ Implement appropriate technical and organizational measures to protect personal data against unauthorized access, loss, or damage
- ☑ Conduct regular security assessments, including vulnerability testing and penetration testing
- ☑ Implement data encryption, pseudonymization, and anonymization techniques where applicable

07. DATA BREACH RESPONSE

- ☑ Develop a data breach response plan to detect, investigate, and report personal data breaches within the specified timeframes
- ☑ Establish procedures for notifying relevant authorities and affected individuals when a data breach occurs

08. PRIVACY NOTICES

- ☑ Create comprehensive privacy notices that inform individuals about the purposes, legal basis, and recipients of their personal data
- ☑ Clearly state the rights of data subjects and how they can exercise those rights
- ☑ Provide contact information for the organization's data protection officer or privacy contact

Data Governance
CHECKLIST

09. DATA PROCESSING AGREEMENTS

- ☑ Review and update data processing agreements with any third parties who process personal data on your behalf
- ☑ Ensure that these agreements include the necessary data protection and security requirements

10. DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)

- ☑ Conduct DPIAs for high-risk processing activities that may result in a high risk to individuals' rights and freedoms
- ☑ Document the assessment process and implement necessary measures to mitigate identified risks

11. EMPLOYEE TRAINING AND AWARENESS

- ☑ Train employees on data protection principles, applicable regulations, and their responsibilities regarding personal data handling
- ☑ Foster a culture of privacy awareness within the organization to ensure compliance at all levels

12. VENDOR MANAGEMENT

- ☑ Assess the privacy practices of third-party vendors and ensure they comply with relevant data privacy regulations
- ☑ Review and update contracts with vendors to include appropriate data protection clauses

13. REGULAR COMPLIANCE AUDITS

- ☑ Conduct periodic audits to assess compliance with global data privacy regulations
- ☑ Document any findings and remediate any identified non-compliance issues

CHAPTER 05

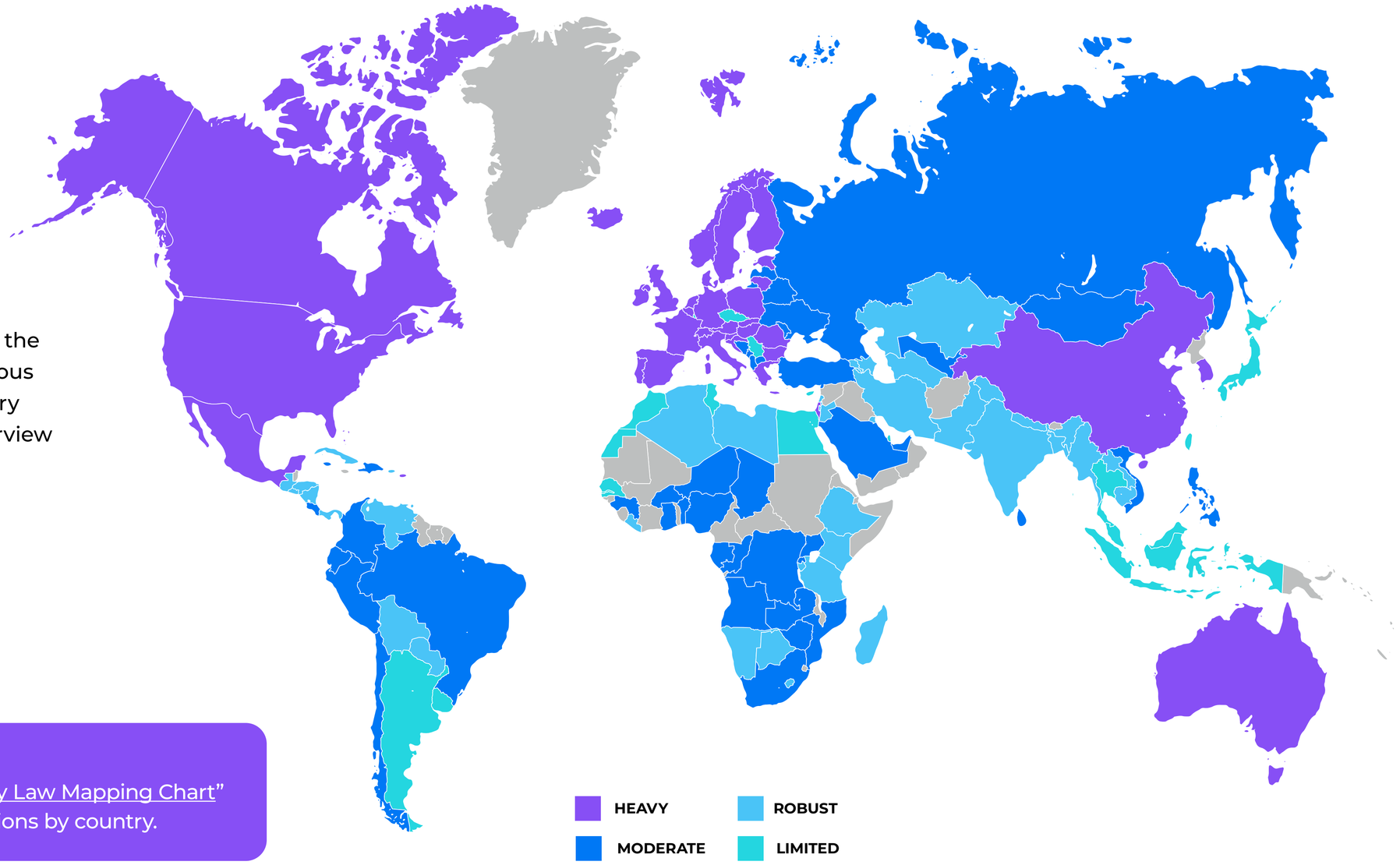
Regional Impacts of Privacy Regulations

Privacy regulations exist all over the world, some of them more robust and wide reaching than others. But any organization that functions on an international level must comply with each and every applicable privacy regulation.

In the future, there will likely be more harmonization of global privacy compliance standards for the collection and use of customer data. Until that time, it is the responsibility of each company to understand their own regional and global privacy obligations. This is why it is critical to have the proper teams, technology, and processes in place to manage data privacy internally, create a solid first party data foundation based on customer consent, and develop the right suite of technology resources to help streamline the management of customer consent. A CDP can be an invaluable asset in these efforts. In fact, Tealium offers the tools and capabilities to comply with multi-jurisdictional privacy governance laws.

Map of Privacy Regs Around the World

The interactive map of global privacy regulations from DLA Piper illustrates the number of regulations impacting various regions around the world. Each country can be clicked on for an in-depth overview of the regulations for each region.



Check out these additional resources:
The IAPP's "Global Comprehensive Privacy Law Mapping Chart" for a robust breakdown of privacy regulations by country.

Global: Data Rights Comparative Table

Privacy Act 1988 & CDR (AU)	Privacy Act 2020 (NZ)	PDPA (SG)	APPI (JP)	PDPO (HK)	PIPL (CN)	GDPR (EU)	CCPA, as amended (CA)
Right to access	Right to access	Right to access	Right to disclosure	Right to access	Right to access	Right of access	Right to know
N/A	N/A - Common law tort of privacy	Right of private action	Right to private action	Right to private action	Right to initiate a private cause of action	Right to private action	Right of private action
Right to correct	Right to correct	Right to correct	Right to correct	Right to correct	Right to correct	Right to rectification	Right to correct
N/A	N/A	N/A	N/A	N/A	N/A	N/A	Right to opt out of the sale of personal information
Forthcoming (Privacy Act); limited right (CDR)	Right to be forgotten	N/A	Limited right	N/A	Limited right	Right to be forgotten	Right to delete
N/A	N/A	N/A	N/A	N/A	Right to decide	Right to restriction of processing	Right to limit the use and disclosure of sensitive personal information
Right to data portability (CDR)	N/A	Forthcoming	N/A	N/A	Right to data portability	Right to data portability	Right to access
N/A	N/A	Right to withdraw consent	N/A	Right to withdraw consent	Right to withdraw consent	Right to withdraw consent	N/A

CHAPTER 06

Industry Impacts of Privacy Regulations

Obviously, data protection laws apply to any business that collects, accesses, or manages personal data, regardless of the industry or sector. Whether it is hospitality, travel, healthcare, finance, retail, or any other industry, businesses must comply with global data protection regulations to ensure the privacy and security of personal information and maintain consumer trust. However, it is true that some industries face more stringent regulations than others due to the sensitivity of the data they are entrusted to manage and access.

06

Managing Customer Privacy in Highly Regulated Industries

Companies operating in highly regulated industries, such as healthcare and financial services, face unique challenges when it comes to managing customer data and ensuring privacy compliance. The types of data they manage, coupled with strict regulations, require a strategic approach to organizing their customer data teams.

In these industries, it is crucial to involve data governance and privacy compliance teams from the outset and maintain ongoing collaboration to ensure compliance with global laws and standards.

Data teams play a central role in managing the CDP and customer data team within highly regulated industries. Given the sensitivity of the data and the importance of compliance, having a dedicated team responsible for overseeing the proper and compliant use of customer data is crucial. Additionally, IT departments can also take ownership of the CDP, given their expertise in managing data infrastructure and ensuring data security.

Marketing departments will also be involved in the ownership of the CDP, as they have a vested interest in maintaining compliance while utilizing customer data to deliver trusted personalized experiences and drive marketing initiatives.

Regardless of the department taking ownership, close coordination with Legal departments is essential. Given the large-scale global privacy requirements faced by organizations in highly regulated industries, the Legal department provides crucial guidance and expertise to ensure adherence to applicable regulations and privacy standards.

Privacy-Enhancing Initiatives in Highly Regulated Industries

01. IMPLEMENTING STRONG ACCESS CONTROLS

Highly regulated industries often deal with sensitive and confidential data. Implementing stringent access controls ensures only authorized personnel can access and handle sensitive information. This includes measures such as two-factor authentication, role-based access controls, and strict password policies, reducing the risk of unauthorized data exposure.

02. CONDUCTING REGULAR SECURITY AUDITS & ASSESSMENTS

Regular security audits and assessments help identify vulnerabilities and potential gaps in data security practices. By conducting comprehensive assessments, you can proactively address any security weaknesses, strengthen their systems, and ensure compliance with industry-specific regulations.

03. ENCRYPTING DATA IN TRANSIT & AT REST

Encryption is a critical privacy measure for protecting data in highly regulated industries. By encrypting data both during transmission and storage, your organization can add an extra layer of security, making it significantly harder for unauthorized individuals to access or decipher the information. Robust encryption protocols, algorithms, and key management systems are vital components of this initiative.

04. IMPLEMENTING PRIVACY-ENHANCING TECHNOLOGIES

Highly regulated industries can leverage advanced technologies to enhance privacy and data protection, many of which Tealium has prebuilt integrations. For instance, implementing data anonymization techniques, such as tokenization or pseudonymization, can help de-identify PII while retaining data utility for analysis and research purposes. Similarly, deploying data loss prevention (DLP) solutions and advanced threat detection systems can help detect and prevent data breaches and insider threats.

CUSTOMER
Case Study

Global Pharmaceutical Organization

Challenge

A global pharmaceutical organization wanted to provide a personalized experience for HCPs and fortify its marketing technology ecosystem for future developments.

Solution

- Indegene and Tealium implemented a bespoke, multi-phased CDP solution that facilitated personalized communications, enhancing engagement and outcomes for HCPs.
- CPRA (California Consumer Privacy Act) and GDPR (General Data Protection Regulation) compliance while capturing and managing HCP data
- Dynamic segmentation based on content affinity and channel preferences
- Automated and near real-time downstream triggers (email, CRM) to support operations for 10+ brands in the United States (US) and European Union (EU)

RESULT

The joint solution created resulted in:

5x
INCREASE
in website conversions

40%
INCREASE
in email open rate

1.5
WEEKS
rapid time-to-market for new brands

Check out these additional resources:
The role of the CDP in Highly Regulated Industries: Gaming
The role of the CDP in Highly Regulated Industries: Banking
The role of the CDP in Highly Regulated Industries: Healthcare

06

Managing Customer Privacy in Less Regulated Industries

In less regulated industries such as retail, travel, and hospitality, organizations still have a responsibility to prioritize and protect customer privacy, even without stringent industry regulatory mandates. Managing customer privacy effectively not only fosters trust but also provides a competitive advantage by delivering exceptional experiences and maintaining a positive brand reputation.

One key best practice is to establish a dedicated privacy team or designate privacy champions within existing departments. This team or individual should be responsible for developing and implementing privacy policies, ensuring compliance with applicable laws and regulations, and regularly assessing and addressing privacy risks. They should also oversee employee training and awareness programs to promote a privacy-conscious culture throughout the organization.

Implementing robust data governance measures is another essential aspect of managing customer privacy. This involves establishing clear guidelines on data collection, storage, access, and usage. Less regulated industries can adopt frameworks such as the GDPR or the CPRA as a reference. By applying these principles, your organization can demonstrate its commitment to privacy and gain a competitive edge.

Privacy-Enhancing Initiatives in Less Regulated Industries

01. IMPLEMENTING DATA ANONYMIZATION TECHNIQUES

By removing or encrypting personally identifiable information (PII) from customer data, your organization can minimize the risk of unauthorized access or unintended exposure. This ensures data is still valuable for analysis and insights while protecting individual privacy.

02. OFFERING TRANSPARENT CONSENT & PREFERENCE MANAGEMENT

Providing your customers with clear and accessible options to manage their own consent and communication preferences is crucial. This allows them to control how their data is used and empowers them to make informed decisions about sharing their personal information. It is critical to have a platform in place to help manage those preferences in real-time, something that Tealium offers.

03. ADOPTING PRIVACY-ENHANCING TECHNOLOGIES

Leveraging technologies such as encryption, tokenization, and secure data transfer protocols helps safeguard customer data during collection, storage, and transmission. Implementing robust cybersecurity measures, including regular vulnerability assessments and proactive threat monitoring, further strengthens data protection.

04. CONDUCTING PRIVACY IMPACT ASSESSMENTS

Regularly assessing the privacy implications of new projects, initiatives, or technology implementations helps organizations identify and mitigate potential risks to customer privacy. This proactive approach ensures that privacy considerations are embedded in the decision-making process.

CUSTOMER
Case Study

Challenge

Amid evolving data privacy regulations and increasing consumer demand for personalization, Kmart sought to grant customers full control over their data, with a centralized consent management solution that enables compliant, personalized experience activation across all channels.

Solution

Tealium uniquely enabled Kmart to develop an innovative centralized consent management solution that unifies a customer's real-time consent status under a single customer profile.

RESULT

200%

INCREASE

Privacy by design unlocked the power of trust to build Kmart's personalization engine. The result was an astounding **200% increase in Kmart's consenting customer base**; in turn, substantially enhancing audience quality for improved relevance and conversions.

Check out these additional resources:

In Data We Trust: Your Guide For Establishing Customer Trust Through Privacy

Video: Future Proofing Your Data Privacy and Compliance Efforts

Teams and Roles Impacted by Privacy Regulations

ROLE	CEO	Marketing	IT	Legal and Compliance
RESPONSIBILITY	The CEO sets the tone for the organization by emphasizing the importance of customer data privacy and making it a company-wide priority.	The marketing department is responsible for ensuring that customer data is collected, stored, and used in compliance with privacy regulations.	The IT department is responsible for creating a framework of a compliant tech stack, properly onboarding appropriate software, implementing robust data security measures, including encryption, access controls, and regular security audits.	The legal and compliance department provides guidance on privacy regulations and ensures that the organization's data practices align with applicable laws.
STEPS TO TAKE	1. Invest in robust security technologies 2. Require privacy training and awareness programs for employees 3. Hire and appoint privacy professionals to oversee data privacy efforts 4. Encourage open communication channels for reporting privacy concerns or incidents 5. Ensure that privacy is considered in all business decisions and processes	1. Design a consent request and management process to obtain and maintain proper consent for data collection and use 2. Ensure transparent communication about privacy practices to customers 3. Implement privacy preferences and opt-out mechanisms to empower customers to control their data 4. Regularly review and update marketing campaigns to ensure compliance with privacy regulations	1. Implement robust data security measures, such as encryption and access controls, to protect customer data 2. Conduct regular security audits and vulnerability assessments to identify and address any weaknesses in data protection 3. Stay updated on emerging threats and security technologies to proactively safeguard customer data	1. Stay current with privacy laws and regulations applicable to the industry and ensure organizational compliance 2. Develop and enforce privacy policies and procedures that align with regulatory requirements 3. Conduct privacy impact assessments and provide guidance on data handling practices to other departments

Teams and Roles Impacted by Privacy Regulations

ROLE	Customer Support	Sales	Product	HR
RESPONSIBILITY	The customer service department interacts directly with customers and must be knowledgeable about the organization's privacy practices, respond to customer requests for data access or deletion, and address any privacy-related complaints or breaches of trust.	The sales team interacts directly with customers and often handles personal information during the sales process. They have a responsibility to handle customer data with care and in compliance with privacy regulations.	The product team plays a role in ensuring that privacy is integrated into the design and development of products and services. They must consider privacy requirements when designing features that involve the collection, processing, or storage of customer data.	The HR department handles employee data, which is also subject to privacy regulations, as well employee access to tools and training on internal policies.
STEPS TO TAKE	1. Train customer support representatives on privacy policies and best practices for handling customer inquiries and data access requests 2. Ensure prompt and appropriate responses to customer inquiries related to data privacy concerns or breach 3. Collaborate with the legal and compliance teams to address privacy-related inquiries or incidents	1. Obtain proper consent for data usage and handle customer data with care during the sales process 2. Educate sales representatives on privacy practices and guidelines for protecting customer data confidentiality	1. Integrate privacy considerations into the design and development of products and services 2. Conduct privacy impact assessments to identify and mitigate privacy risks associated with new features or enhancements 3. Follow privacy-by-design principles and ensure that privacy controls are embedded in the product's functionality	1. Implement policies and procedures to protect employee data privacy and ensure compliance with applicable privacy laws 2. Provide privacy training and awareness programs to employees, emphasizing their role in safeguarding customer and employee data 3. Establish proper access controls and data handling practices for employee data to minimize the risk of unauthorized access or disclosure

How Technology and Tealium Can Help

Safeguarding customer data privacy is of paramount importance. As organizations strive to comply with stringent global data privacy regulations and build trust with their customers, a Customer Data Platform becomes a vital platform to enable this.

According to our State of the CDP 2023 survey of 1,200 CDP users around the world, 95% of organizations with four years or more of CDP experience were confident in their ability to comply with new privacy regulations.

In today's privacy-conscious world, a CDP is no longer a nice-to-have part of your tech stack, but a MUST-have for organizations seeking to protect customer data privacy. Tealium's market leading CDP offers a comprehensive solution that encompasses data governance, legal compliance, and seamless integration with privacy-related technologies.

Building a solid foundation for privacy-centric data management will not only ensure your compliance with global privacy regulations, it will also foster customer trust and open up competitive advantages that will propel your organization forward even as privacy regulations continue to evolve and expand worldwide. This is why hundreds of global businesses trust Tealium as their partner in safeguarding their customer data while helping them to unlock the full potential of their customer data.

95%

of organizations with four years or more of CDP experience were somewhat or very confident in their ability to comply with privacy regulations.

Only 67% of companies without a CDP expressed confidence in their privacy compliance.

How Technology and Tealium Can Help

The Role of Tealium's CDP in Customer Data Privacy

Tealium's CDP plays a pivotal role in safeguarding customer data privacy. Acting as a centralized platform, we empower organizations to manage and secure customer data while complying with data privacy regulations. With our robust data governance framework, our customers can exercise granular control over customer data access, consent management, and data retention policies. This ensures customer data is handled in a secure and compliant manner, protecting privacy and fostering trust with customers.

Tealium's Competitive Edge: Going Beyond Privacy Compliance

We offer a comprehensive customer data management solution that covers a wide range of privacy-related needs. Our CDP serves as a certified technology foundation, providing organizations with a solid infrastructure to build their privacy-centric data management practices upon. What sets us apart is our commitment to signing Business Associate Agreements (BAA), reinforcing the legal framework for data security and compliance. With Tealium, our customers can have the peace of mind that their customer data is protected.

Enabling Privacy Excellence Through Seamless Integration with Privacy-Related Technologies

At Tealium, we understand that no organization operates in isolation. That's why our CDP is designed to seamlessly integrate with other top-tier privacy-related technologies such as OneTrust, TrustArc, Usercentrics, and Didomi. We empower our customers to leverage the best privacy practices and tools available on the market. By partnering with Tealium, your organization can build a robust privacy ecosystem, fortified by our seamless integration capabilities.

Data Privacy Terminology

Anonymization: The process of removing or altering identifiable information from data sets to prevent the identification of individuals.

California Privacy Rights Act (CPRA): A comprehensive data protection law in California that grants residents certain rights and imposes obligations on businesses regarding the collection and processing of personal information. It aims to enhance consumer privacy rights, transparency, and control over personal data.

California Privacy Rights Act (CPRA): An amendment to the California Privacy Rights Act (CPRA) that enhances consumer privacy protections, introduces new obligations for businesses, and strengthens individual rights regarding personal information.

Consent: Voluntary, informed, and specific agreement given by an individual for the collection, processing, and sharing of their personal data.

First Party Cookie: A small text file stored on a user's device by the website you visit, allowing it to remember user preferences and provide a personalized browsing experience.

Third Party Cookie: A small text file stored on a user's device by domains other than the website you're currently on, allowing those domains to collect data for various purposes, including advertising and analytics.

Cross-Border Data Transfer: The transfer of data from one country to another, often subject to specific legal requirements and safeguards.

Data Aggregation: The process of collecting and combining various data points to create a comprehensive view or analysis of a particular topic or group of individuals while preserving anonymity.

Data Anonymization: The process of removing or modifying personal data in a way that it can no longer be attributed to an identifiable individual.

Data Breach: The unauthorized access, acquisition, or disclosure of personal data, leading to a potential risk to the rights and freedoms of individuals.

Data Breach Notification: The process of notifying individuals, authorities, and other stakeholders in the event of a data breach that poses a risk to personal data.

Data Controller: The entity or organization that determines the purposes, means, and methods of processing personal data.

Data Encryption: The process of transforming data into a coded form to protect it from unauthorized access or interception.

Data Ethics: The study and application of ethical principles and practices in the collection, use, and handling of data, ensuring responsible and fair treatment of individuals and their information.

Data Masking: The technique of replacing sensitive data with fictional or obfuscated data to protect its confidentiality during testing or development.

Data Minimization: The principle of collecting and processing only the minimum amount of personal data necessary for a specific purpose.

Data Portability: The right of individuals to receive their personal data from a data controller in a commonly used and machine-readable format and, if technically feasible, to transmit that data to another data controller.

Data Privacy: The protection and appropriate handling of personal data, ensuring that individuals have control over how their information is collected, used, and shared.

Data Processor: An entity or organization that processes personal data on behalf of the data controller, following their instructions.

Data Protection Impact Assessment (DPIA): A systematic evaluation of the potential risks and impacts on individual privacy and data protection that may arise from a specific data processing activity.

Data Protection Officer (DPO): A designated person within an organization responsible for overseeing data protection and ensuring compliance with privacy laws and regulations.

Data Retention: The period for which data is stored and maintained by an organization before it is securely deleted or destroyed.

Data Sovereignty: The concept that data is subject to the laws and regulations of the country or region in which it is collected and stored.

Data Subject: An individual who is the subject of personal data and has rights and control over how their data is processed.

Data Subject Access Request (DSAR): A request made by an individual to a data controller to exercise their rights regarding the access, rectification, erasure, or restriction of their personal data.

GLOSSARY

Data Subject Consent Management: The practice of obtaining, managing, and documenting individual consent for the collection, processing, and sharing of their personal data.

Data Subject Rights: The various rights granted to individuals regarding the processing of their personal data, including rights such as access, rectification, objection, and restriction of processing.

Data Transfer: The movement or transmission of personal data from one location or entity to another, often across international borders.

De-identification: The process of removing or modifying personal data in a way that it can no longer be linked to an identifiable individual.

First Party Data: Data collected directly from individuals by the organization that intends to use it for its own purposes, such as data collected through website interactions or customer surveys.

General Data Protection Regulation (GDPR): A comprehensive data protection regulation implemented in the European Union (EU) that sets guidelines for the collection, processing, and transfer of personal data.

Opt-in: The act of actively providing consent or choosing to participate in a particular activity or data processing operation.

Opt-out: The act of choosing not to participate or withdrawing consent for a particular activity or data processing operation.

Personal Data: Any information relating to an identified or identifiable individual, such as name, address, email, phone number, etc.

Personally Identifiable Information (PII): Information that can be used to identify an individual, such as name, address, social security number, or email address.

Privacy by Design: The concept of incorporating privacy measures and protections into the design and development of systems, products, and services from the outset.

Privacy Compliance: The practice of ensuring that an organization's data processing activities align with applicable laws, regulations, and industry standards related to privacy and data protection.

Privacy Impact Assessment (PIA): A systematic assessment of the potential privacy risks and impacts of a project or initiative involving the collection and processing of personal data.

Privacy Notice: A statement or document that informs individuals about the collection, use, and sharing of their personal data by an organization.

Privacy Policy: A document that outlines an organization's practices and procedures regarding the collection, use, and sharing of personal data.

Privacy Shield: A framework that provided a legal mechanism for transferring personal data between the European Union and the United States, ensuring an adequate level of data protection. It was invalidated by the European Court of Justice in 2020.

Pseudonymization: The process of replacing identifying information with pseudonyms to protect the privacy of individuals while allowing data analysis and processing.

Right to Access: The right of individuals to obtain confirmation from a data controller whether their personal data is being processed and, if so, to access that data.

Right to Erasure: Also known as the "right to be forgotten," it allows individuals to request the deletion or removal of their personal data.

Second Party Data: First-party data collected by one organization and shared with another organization for joint marketing efforts or other collaborative purposes.

Sensitive Data: Data that requires additional protection due to its highly personal or confidential nature, such as financial information, medical records, or biometric data.

Third Party Data: Data collected by an entity or organization that is separate from the organization using the data. This data is often obtained from external sources such as data brokers or public records.

Tracking Technologies: Technologies used to monitor and track user behavior online, such as pixel tags, web beacons, or device fingerprinting.

Zero Party Data: Data that is willingly and proactively shared by individuals with an organization, typically through interactions, surveys, or preference centers. This data is provided directly by the individuals themselves and can include preferences, intentions, or interests.

This report was published by

TEALIUM®

Tealium connects customer data across web, mobile, offline and IoT so businesses can better connect with their customers. Tealium's turnkey integration ecosystem supports more than 1,300 built-in connections, empowering brands to create a complete, real-time customer data infrastructure. Tealium's solutions include a customer data platform with machine learning, tag management, an API hub and data management solutions that make customer data more valuable, actionable, privacy-compliant and secure. More than 850 leading businesses throughout the world trust Tealium to power their customer data strategies.

For more information, visit

tealium.com