IN DA*A WE TR*ST

A Guide for Establishing Customer Trust Through Privacy

TEALIUM®

Foreword 3

Introduction 4

The History of Data Privacy Regulation 5

- Timeline of Data Privacy changes to Digital Marketing 6
- Complex Customer Data Needs Require Simple, Flexible Solutions 8
  - 5 Ways a CDP Establishes Trust in Data with Customers 9
- How Can Privacy by Design Be Done by Organizations at Scale? 11

The Anatomy of a Customer Data Platform 12

- How Tealium's Product Offerings Support Privacy Management and CX Personalization 13

Customer Trust Must Go Beyond Marketing 14

- Key Roles and Departments for the New Customer Data Strategy 15
  - The Data Center of Excellence 16
  - Highly Regulated Organizations 17

Three Key Recommendations for Establishing Customer Trust Through Data 18

- Make Privacy Purposeful 18
- Give Customers a Reason to Opt-In 20
- Map Out a Customer Journey 23

Why Companies Around the World Trust Tealium 26

- Tealium's Role in a Privacy and Consent Initiative 27
  - Consent Acquisition 28
  - Consent Management & Orchestration 29
- Engineered for Scale and Reliability 30

Foreword

Privacy is now a top consideration and focus for organizations. Any business that is data-driven, that requires personal data to be processed, needs to prioritize data privacy and have a thoughtful perspective on how data is collected and used.

Data privacy across the globe varies, so it's important to understand the different regulations. Europe has the General Data Protection Regulation (GDPR), the US has the California Consumer Privacy Act (CCPA) soon to be the California Privacy Rights Act (CPRA). Japan and Australia also have their own federal regulations. All privacy regulations constantly evolve due to regulators sharing insights into enforcement cases, as well as sharing guidelines to explain how compliance is achieved. Therefore, it can be challenging for a business to respond and be adequately prepared.

All major privacy regulations put the consumer in the driver-seat, letting them to decide what data they want to share. Consumers may, therefore, provide less personal data, but at the same time expect an organization to deliver relevant and personalized experiences.

This is a challenge for all businesses: to have a benefit-driven conversation with customers, led by privacy.

One strategy modern organizations are adopting includes having a privacy-first data strategy. A key technology component of the strategy is a Customer Data Platform. CDPs help ensure the right data is collected and activated across respective channels - and importantly that privacy preferences are upheld throughout the process. Historically, customer data included purchase history and actions on a webpage. Now there is significantly more data available to collect, which means companies need to identify quality data and respect the end users' privacy preferences. CDPs help companies deliver the right type of content, offer, and information at the right time for the buyer. This helps build a trusted relationship with the buyer, which is especially critical today.

The CDP is becoming a staple in the majority of companies because teams can orchestrate required privacy preferences, add or remove vendor activations, change the implementation, and modify what events are shared.

Even with the evolving state of privacy regulations and new ways customer data needs to be handled, businesses can deliver great experiences and moments that delight their customers. This book will cover the fundamentals in a manner that is concise and actionable. It can feel daunting, but we are here to help. Our goal is to distill the complex, so teams can get started now with the right technology to support a privacy-first data strategy.

– Julian Llorente Perdigones, Director of Data Privacy at Tealium

Introduction

In today's data and privacy-driven world, it is imperative for businesses to provide clarity to their customers on why, how, and what personal data they want to process and share with third parties. This is not only required to comply with ever-evolving privacy regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), but it's also a necessity for establishing trusted customer relationships. When you provide your customers with a relevant and helpful experience in exchange for their data, their trust in your business is strengthened as is their loyalty to your brand. So while acquiring their consent and complying with privacy laws is a great start, it's even more important that you use customer data to benefit your customers by delivering amazing and trusted experiences.

Consumers Value Digital Trust
Consumers report that digital trust truly matters – and many will take their business elsewhere when companies don't deliver it.

Companies Need to Establish Trust Today

As in every relationship, you have to establish credibility before a person trusts you. This is no different from the relationship between businesses and consumers. Today, many companies utilize value exchange models where companies provide something beneficial in return for customer data e.g. email address for 50% off an item. Consumers understand their information is being collected and tracked, but they expect a trusted experience with the brand. To enable this, businesses require a trusted partner and supporting technology that will help provide the foundation for privacy-driven collection, transformation, orchestration, and activation of customer data.

There are Costs if Trust is Not Established and Maintained

Brands benefit from maintaining customers' trust, but can also incur significant costs when it's lost. When customers spend money with a brand, they're relying on the service or product they have purchased to meet certain expectations of quality. Likewise, when a customer provides data to a brand, they expect the brand to use that data responsibly. In both cases, the outcome is a high price tag: **71% of PwC's study respondents said they would buy less from a business that lost their trust.** Out of that, **73% said they would spend significantly less.** Customers want to trust brands they like and as our research reveals, once that trust is lost, it is nearly impossible to regain — **85% of customers won't forgive a company's missteps, even if they previously trusted the brand.**

The History of Data Privacy Regulations

In the digital era, we share more personal information than ever before. Whether through social media, online dating, or even just a simple Google Search - our private data is out there in the world.

One of Tealium's partner integrations, Sailthru, a cross-channel marketing platform, recently conducted a survey that found "**81% of respondents cited a willingness to share personal data to earn loyalty program benefits** to a trusted retailer/brand and **70% are willing to share their data to receive special discounts** and offers to a trusted brand/retailer."

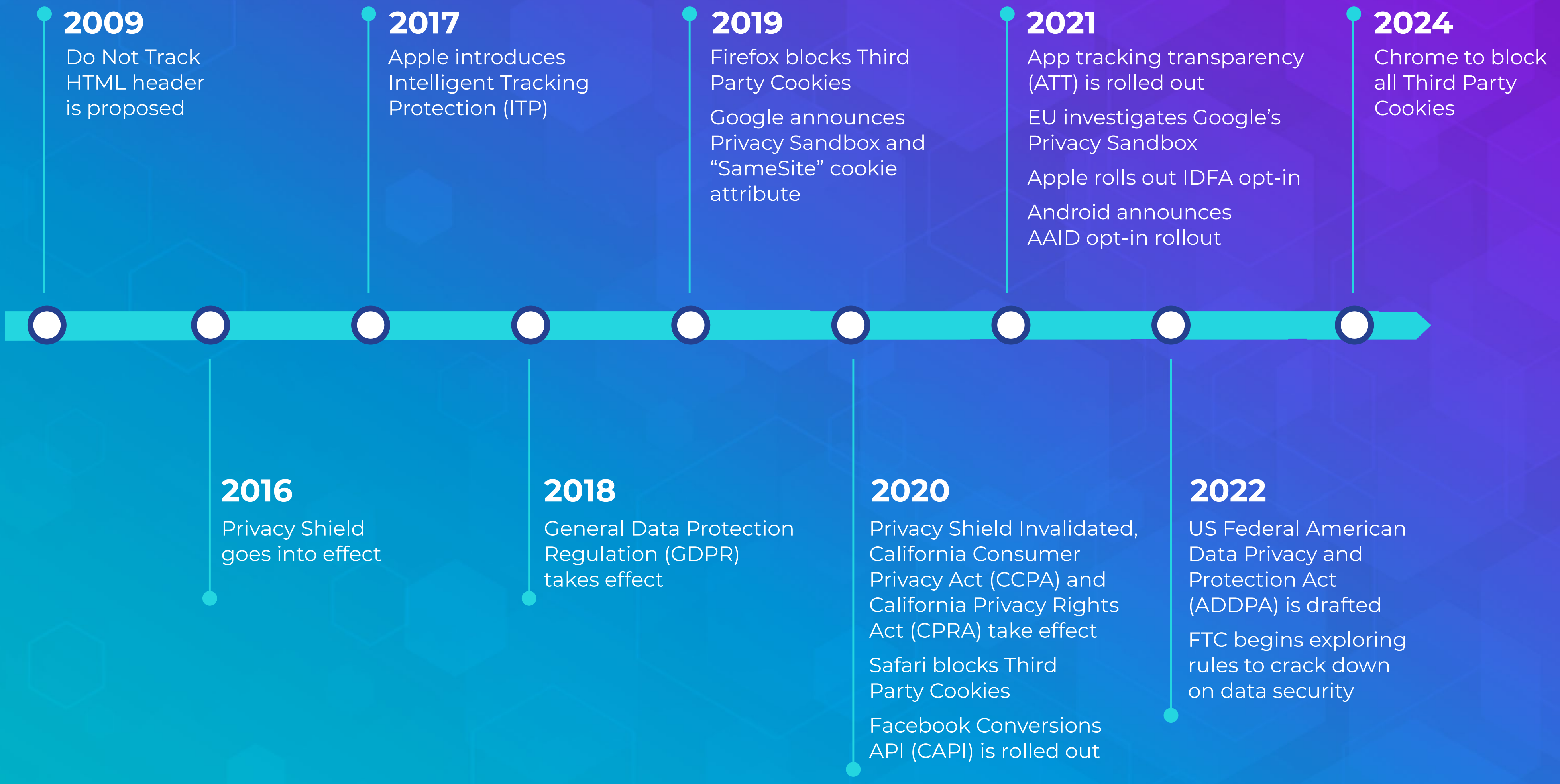
Sharing personal information with companies we interact with enables meaningful personalization that makes an impact on our daily lives - exposure to medical knowledge based on real-time health analysis, financial advice based on lifestyle and spending habits, product offers that reflect our unique individuality, and customized experiences that take travel or entertainment to the next level (to name only a few).

The two most important factors for a trustworthy digital relationship between a customer and a brand are transparency and value.

This entails articulating how customer data will be processed and for which purpose, using clear language that all customers understand. Data-driven companies must establish an effective Data Strategy to address this challenge, whose goals are focused on understanding the value of customer data, and the inherent responsibilities in its effective stewardship.

Before the introduction of GDPR in 2018, companies had historically been collecting data for marketing purposes, but without customer consent. Certainly, cookie banners and privacy policies were fairly well recognized by this time, but the frameworks were all different and there were no industry nor legal standards in place that could assist the customer in understanding why a Value Exchange was important. In order to opt-out of advertising in those years, customers were forced to follow links to external third party systems which allegedly would remove them from some nascent audience advertising with hundreds of different technology vendors whose names most people did not know, nor understood what they did. **It was this environment of perplexity that ushered in the first, most important step of institutionalizing privacy regulations: acquiring and managing consent.**

Timeline of Data Privacy Changes to Digital Marketing



2009
Do Not Track HTML header is proposed

2016
Privacy Shield goes into effect

2017
Apple introduces Intelligent Tracking Protection (ITP)

2018
General Data Protection Regulation (GDPR) takes effect

2019
Firefox blocks Third Party Cookies

Google announces Privacy Sandbox and “SameSite” cookie attribute

2020
Privacy Shield Invalidated, California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) take effect

Safari blocks Third Party Cookies

Facebook Conversions API (CAPI) is rolled out

2021
App tracking transparency (ATT) is rolled out

EU investigates Google’s Privacy Sandbox

Apple rolls out IDFA opt-in

Android announces AAID opt-in rollout

2022
US Federal American Data Privacy and Protection Act (ADDPA) is drafted

FTC begins exploring rules to crack down on data security

2024
Chrome to block all Third Party Cookies

The requirements for consent have required businesses to detail what data they want to process, for which purpose, and with whom they're going to share it while allowing the customer to decide whether or not they want to opt-in to such activities. This means the customer has gained the power (and rightly so) to decide how and when their data will be used.

> This transparency on how customer data will be leveraged creates a foundation of trust and companies that embrace this strategy will develop trusted relationships with their customers and will ultimately have a competitive edge now and in the future.

As the industry moves forward with new innovations in AI technologies, digital marketing, and customer engagement techniques, customer data has become the foundational element that will determine the level of success that can be realized. Consent is the key to unlocking the full potential of our investments in new innovation, allowing businesses to use customer information to power modern services and experiences throughout a customer journey that involves an omnichannel of devices and systems, all of them with different needs for personal data protection and brand marketing.

In the following sections, we will take a closer look at how Customer Data Platforms (CDPs), and specifically Tealium's CDP, turn privacy and customer trust into a strategic advantage. We offer real-world tips from privacy experts and marketers on how to boost the transparency required for privacy by design. We clarify who is now responsible for collecting and protecting customer data, outline the ideal privacy team, and approach necessary to tackle the complexity of privacy regulations around the world.

Complex Customer Data Needs Require Simple, Flexible Solutions

Customers expect the brands they interact with to understand them, know who they are, and ultimately provide an optimal user experience. While on the other hand, they also expect brands to respect their data privacy rights which are now officially documented and enforced around the world. This is often referred to as the “Privacy Paradox.”

The Privacy Paradox

The inconsistency between customer concerns over privacy and their actual online behavior and desires has been coined “the privacy paradox” by Gartner.

On the one hand, according to a survey conducted by one of our partner integrations, Merkle, “**88% of consumers view a brand’s products as having higher quality** if they feel like the brand is listening to their needs. 91% of consumers are slightly or significantly likely to make a repeat purchase if they feel a brand has listened.” On the other hand, according to research conducted by the Pew Research Center, “**81% of the public say that the potential risks they face because of data collection** by companies outweigh the benefits.” And “**79% of consumers are concerned** about how companies use the data collected.”

In order to collect, enrich, and activate customer data in a way that simultaneously meets privacy compliance requirements while delivering amazing experiences, companies require a flexible and vendor-agnostic solution that will integrate across their entire Martech stack - the solution is a Customer Dvata Platform (CDP).

A CDP can sit at the center of your data supply chain and help you manage your customer data and data privacy at the same time. It is possible to deliver great experiences and uphold privacy preferences!

The Privacy Paradox in Numbers

91% of consumers are slightly or significantly likely to make a repeat purchase if they feel a brand has listened to their needs.

81% of the public say that the potential risks they face because of data collection by companies outweigh the benefits.

5 Ways a CDP Establishes Trust in Data with Customers

1 Reduce Risk from Siloed Data

Data silos result in costly processes and increased risk in multiple areas, such as duplication, stale datasets, and erroneous or fractured understandings of customer profiles that lead to wasted marketing budgets and flawed strategies. These silos keep your organization from maximizing your customer experience and can also put you at risk of privacy infractions. If one department manages customer data differently than another, your teams are speaking different languages and missing requests for ongoing data privacy management. A CDP that starts with data collection will help your organization remove these data silos and reduce your risk of non-compliance.

2 Propagate Privacy Preferences

If your consent data is not real-time, you open your organization up to risk and can even inadvertently breach privacy regulations while consent preferences may be in queue to be updated. For example, if someone requests their data to be deleted and it takes your organization longer than is legally mandated to fulfill that request, your organization can face significant penalties for non-compliance with Data Subject Access Requests. Therefore, it is critical for privacy to be propagated throughout the entire customer journey, across all channels, and maintained through the lens of the customer. Privacy compliance maintained by channel is not actually compliant, and fraught with risks of infraction.

3 Enable Operational Efficiency and Business Agility

To be a privacy-driven organization, businesses must break down communication and data silos to understand what data is being processed and why. Tealium's CDP enforces a common nomenclature for data, allowing the business and IT units to speak one common language consistently. This universal schema of data eliminates any risk of one department falling behind another whenever privacy requirements change or new technology investments call for new integrations.

5 Ways a CDP Establishes Trust in Data with Customers

4 Give Customers Transparency and Control Over Their Data

Your customers are empowered by global privacy regulations to manage when their data is collected, stored, and utilized. A CDP becomes a trusted repository of customer data and the governed supply chain that connects customer devices to the platforms that deliver value. As a trusted steward of their data, your customers will have access to the most accurate and meaningful set of their personal data when they request it, and supporting systems like Consent Management Platforms help supplement the CDP overseeing the collection and orchestration of that data.

5 The Ultimate Customer Experience

A CDP can help organizations better understand customer behavior and preferences through a single customer view. Customers want to be known and understood regardless of what device they use or whether they are engaging in-person or online. Today, companies often have customer data residing in different systems e.g. social and email platforms. Additionally, a customer may have different privacy settings for each of those platforms which could result in privacy preferences not being respected. CDPs can enable you to collect trusted customer data from all touchpoints to produce a unique 360 view of your customers which will be your foundation for all things privacy-related. This enables you to create real-time engagement on any channel based on customer preferences. And this level of personalization can be done at scale through a vendor-neutral, real-time CDP like Tealium.

How Can Privacy by Design Be Done by Organizations at Scale?

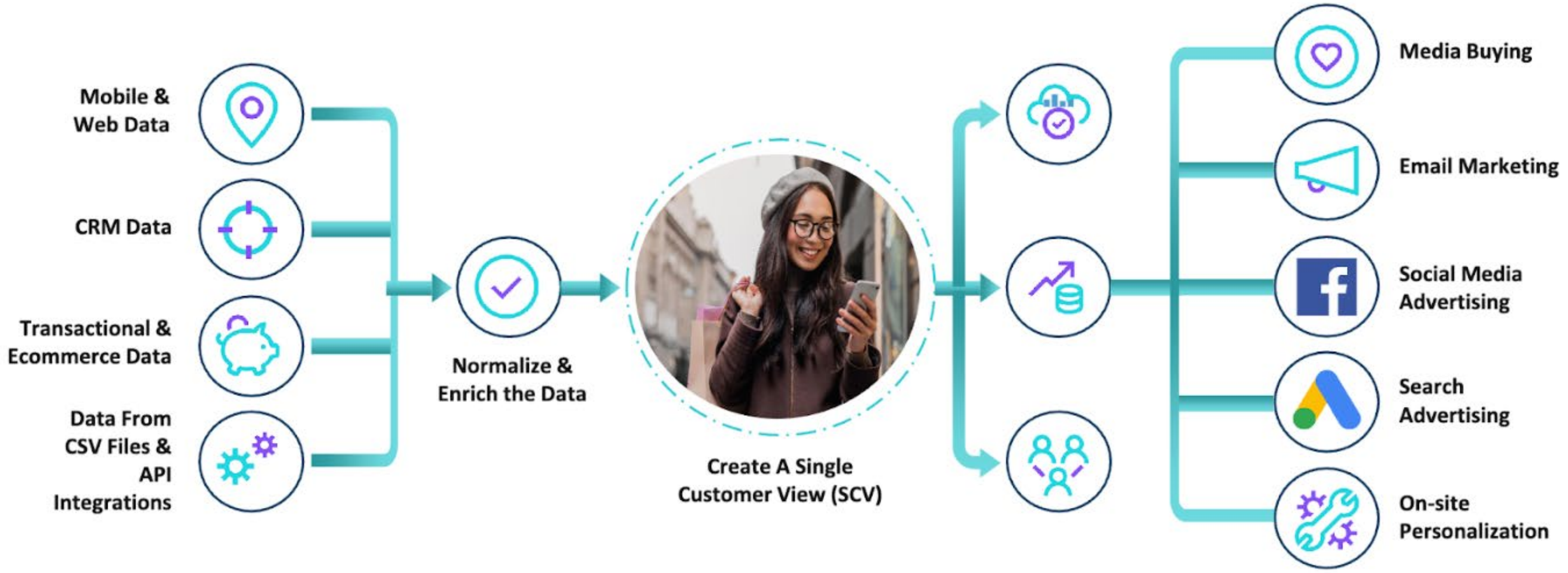
Privacy by design is the method of designing data privacy into all your business processes and operations so that Personally Identifiable Information (PII) is protected by default. Data governance is the formal, documented policy for managing the availability, usability, integrity, and security of the data in enterprise systems, based on internal data standards and policies defined through privacy by design. In order to achieve the proper management of privacy and personalization at scale, an organization must onboard a suite of technology solutions that align with both the parameters of privacy by design and the processes defined through data governance. A Customer Data Platform is ideal for this unified approach.

Some of the primary systems required for implementing Privacy by Design and data governance include:

- **Consent Management Platform (CMP):**
  Collect consent data and implement privacy processes such as Data Subject Access Requests.
- **Cross-Channel Marketing Tool:**
  Connect to your customers across platforms with privacy principles incorporated in the chosen channel integrations.
- **Behavioral and Experience Analytics:**
  Understand and build better digital experiences by considering privacy preferences throughout the customer engagement and adjusting the experience to the most optimal level permitted by the consumer.
- **Customer Data Platform (CDP):**
  Build an independent data foundation that your facilitating technologies can rely upon to fuel their data needs and orchestrate data delivery in a trusted fashion.

> “Putting the CDP at the center of the privacy strategy gives us one place to control the data that our organization accepts responsibility for, and allows us to consistently understand the data lineage that we should be stewards of.”
>
> *- Ted Sfikas*
>
> *Senior Director of Value Engineering*
> *& Digital Strategy at Tealium*

The Anatomy of a Customer Data Platform


Mobile & Web Data
CRM Data
Transactional & Ecommerce Data
Data From CSV Files & API Integrations
Normalize & Enrich the Data
Create A Single Customer View (SCV)
Media Buying
Email Marketing
Social Media Advertising
Search Advertising
On-site Personalization

The above technologies help provide a way for companies to govern data at scale. It is critical for data to be governed from the moment it is collected to the moment it is activated throughout the technology stack, without disrupting the current architecture or requiring unreasonable financial investments.

Tealium's CDP platform was designed with a Data First philosophy, meaning it starts at the point of data collection. Specifically, Tealium provides the technologies that automate necessary governance with data collection automation (Tealium Data Connect, Tealium iQ Tag Management, and Tealium EventStream API Hub), Customer Profile creation and enrichment (Tealium AudienceStream CDP), and Customer Data Analytics and Reporting (Tealium DataAccess and Tealium Data Insights).

How Tealium's Product Offerings Support Privacy Management and CX Personalization, from Tag Management to CDP

Tealium Data Connect

When customer data resides on key business systems like Data Warehouses, Data Lakes, MDMs, and other important repositories that are part of the data supply chain, it is critical to unify and validate these datasets prior to onboarding it to the CDP so that it is fit for use. Data Connect provides a visual interface to efficiently achieve this goal and allows for consistent governance to take place in an automated fashion.

Tealium Event Data Framework

Governance is highly optimized when real-time customer data is collected in the form of Events, which are any customer interaction with your brand, in-person or online, that is counted as a unique data point that should be incorporated into a customer profile. Events represent the unit of measurement for customer interactions to give you a granular view of customer behavior and ensure the right data is detected and collected in the right format, making it immediately usable for all systems. Events represent information that is meaningful to the business systems that are being relied upon to take action, delivering modern customer experiences while respecting privacy, and allowing the business to easily gain insights through intuitive reporting capabilities. Tealium collects and activates these Events in real-time, on any device that surfaces them, using the Event Data Framework, a package of data collection technology that rapidly and effectively deliver on these needs:

- **Tealium iQ Tag Management (TiQ):** Tag Management Systems are the industry standard to designing and activating Event Data on websites. TiQ is a Device-Based approach to governing and automating Event Data on websites, leveraging pre-built Javascript Tags to enforce Consent and subsequent activation as required. TiQ's automation takes place directly on customer devices like mobile phones and browsers.
- **Tealium EventStream API Hub:** To overcome modern browser-based restrictions that are intended to support Privacy mandates, Tealium EventStream is used to provide the same capability of governance and automation as TiQ, but instead uses a Cloud-based approach to collect and govern the Event Data. EventStream first places the collected data into a Cloud environment for validation and enrichment, and then activates the data securely to any destination via APIs.

Both approaches to real-time customer data management fulfill the privacy and marketing needs of governing customer data in a secure fashion, via a proven Event-driven model that has become the industry standard today.

Tealium DataAccess and Data Insights

Measurement and Insights have become key to continuous improvement of Marketing teams and IT initiatives alike. With DataAccess and Data Insights, the modern Incrementality and Experimentation strategies that will be necessary to compete are delivered to existing Business Intelligence departments without additional investments in new solutions. Tealium supports the chosen BI tools of the business to deliver dashboards, reports, and segmentation services that new innovations will require in order to be optimized, such as Data Clean Rooms that may be included for future media strategies and Media Mix Modeling.

Customer Trust Must Go Beyond Marketing

It's long been held that marketing takes a leading role in attracting, engaging, and maintaining a trusted relationship with customers. As more data has become available and buyer expectations have risen, marketing teams have invested in CDPs as a way to drive richer customer experiences. **CDPs enable many types of marketing use cases by simplifying the tracking of data, standardizing the data throughout different data sources, and integrating in real-time with designated partners** like Meta, Google, and others, to offer cutting-edge and meaningful customer experiences.

Yet, with the introduction of GDPR and the proliferation of privacy regulations around the globe, the responsibility for establishing customer trust through data has established a new incentive for all teams - not just marketing. Data-driven businesses have every reason to invest heavily in data clarity (the understanding of what data is being processed, by who, and for which purposes) as it leads to new revenue streams and improves costly operational processes. This incentive is not only valued by Marketing; it also applies to Data Science, Product, Business Intelligence, Sales, and Customer Success teams as well, making it a key component of the entire organization's customer strategy.

So how does the subsequent reallocation of responsibilities for this unified strategy impact the organization? **While all employees in the organization need to understand customer data policies and procedures, there are a few departments and roles that work directly on these efforts independently**. The approach becomes more aligned with a proven Center of Excellence approach.

Key Roles and Departments for the New Customer Data Strategy

Data Privacy Professionals

The Compliance of Data

With all the global data privacy regulations, data privacy experts are now a major player in onboarding a CDP. This includes Chief **Information Security Officers (CISO), Chief Privacy Officers (CPO), Data Privacy Managers, Analysts, and more**, who will be responsible for developing and implementing privacy programs across the organization. They are also responsible for working with the rest of the data team to establish the right internal data governance policies and procedures to break down internal silos and ensure the right data is being collected and managed from an analytics and privacy perspective. These individuals must work closely with the tech and marketing teams on privacy enforcement and compliance to ensure your organization meets and manages regulatory and contractual obligations in a privacy-sensitive manner.

Marketer

The Customer Experience of Data

Marketers are on the front lines of data privacy and developing a trusted relationship with customers. This team of individuals, including the **Chief Marketing Officer (CMO), Marketing Channel Managers, Marketing Operations, and more**, engage with customers, facilitate the collection of data, and activate it. They're the ones tasked with delivering on the responsibility of obtaining customer consent. Therefore Marketing plays an active role with the privacy team and developers to determine how data is going to be collected and how privacy preferences will be respected.

They must work with the tech teams who manage the Martech stack as well as the data teams to ensure they are following the established data governance policies, the analytics are supporting their marketing activities, and ongoing privacy requirements are being adhered to and updated as needed in marketing campaigns.

Hybrid Roles -

The Marriage of Data Responsibilities

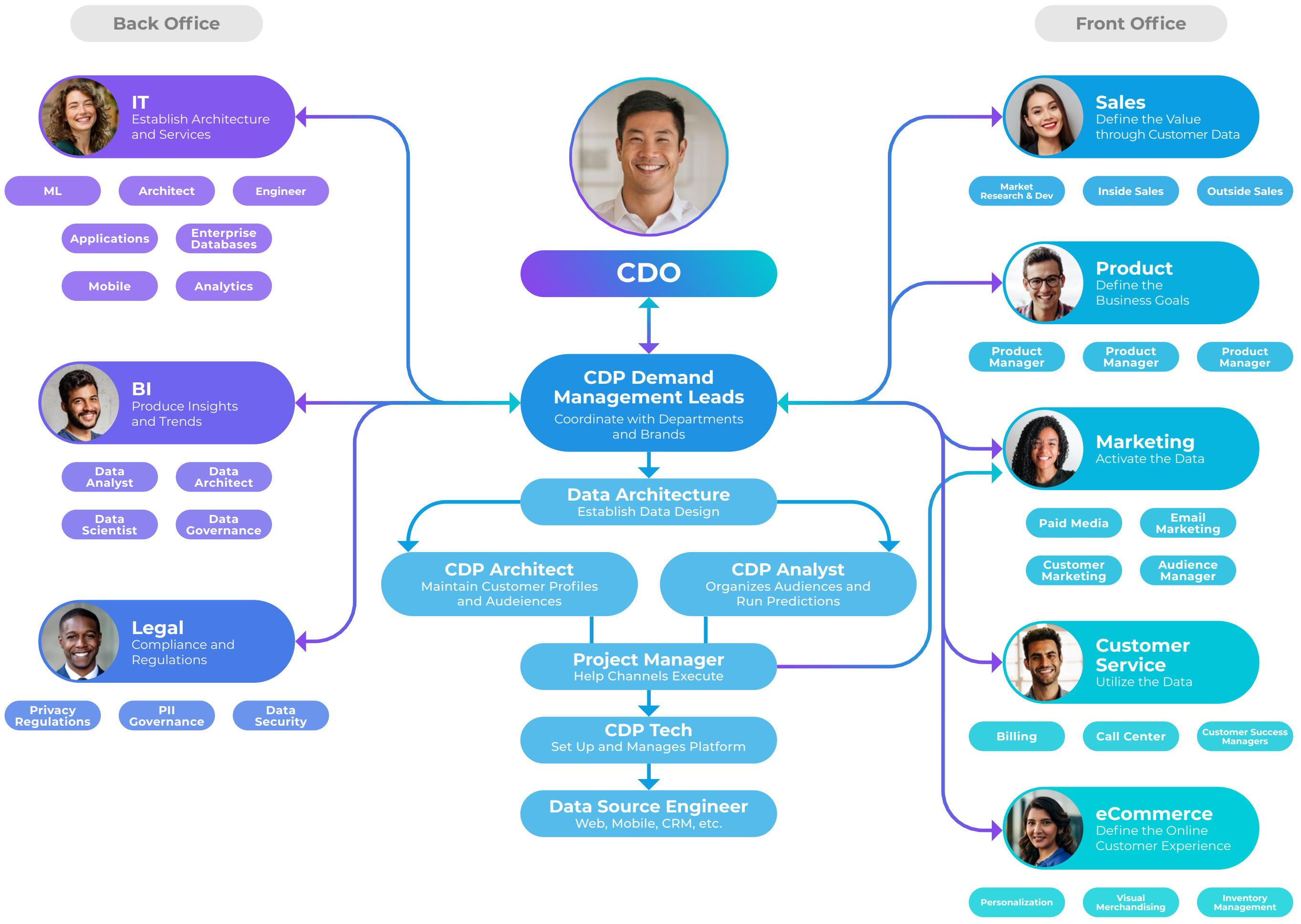
In our recent eBook, "The Organization of the Future," we explain how roles within the enterprise have shifted due to the growing importance of customer data management and the adoption of CDPs. There is also an emergence of new executive leadership roles, such as the Chief Data Officer, who is aligned with Security and Infosec stakeholders to own the responsibility of data stewardship in concert with the more traditional roles that have always governed data in a broad sense.

Due to the ongoing evolution of data privacy and its role across the organization, new hybrid roles are emerging that manage the cross-functional nature of privacy and personalization

Some of these roles include:

- **Privacy Marketer**
- **Privacy product marketing managers**
- **Privacy engineers who map out privacy by design**
- **People who are a bridge who can speak both languages and can attain the clarity needed**

The Data Center of Excellence



Back Office

Front Office

CDO

IT
Establish Architecture and Services

ML

Architect

Engineer

Applications

Enterprise Databases

Mobile

Analytics

BI
Produce Insights and Trends

Data Analyst

Data Architect

Data Scientist

Data Governance

Legal
Compliance and Regulations

Privacy Regulations

PII Governance

Data Security

CDP Demand Management Leads
Coordinate with Departments and Brands

Data Architecture
Establish Data Design

CDP Architect
Maintain Customer Profiles and Audeiences

CDP Analyst
Organizes Audiences and Run Predictions

Project Manager
Help Channels Execute

CDP Tech
Set Up and Manages Platform

Data Source Engineer
Web, Mobile, CRM, etc.

Sales
Define the Value through Customer Data

Market Research & Dev

Inside Sales

Outside Sales

Product
Define the Business Goals

Product Manager

Product Manager

Product Manager

Marketing
Activate the Data

Paid Media

Email Marketing

Customer Marketing

Audience Manager

Customer Service
Utilize the Data

Billing

Call Center

Customer Success Managers

eCommerce
Define the Online Customer Experience

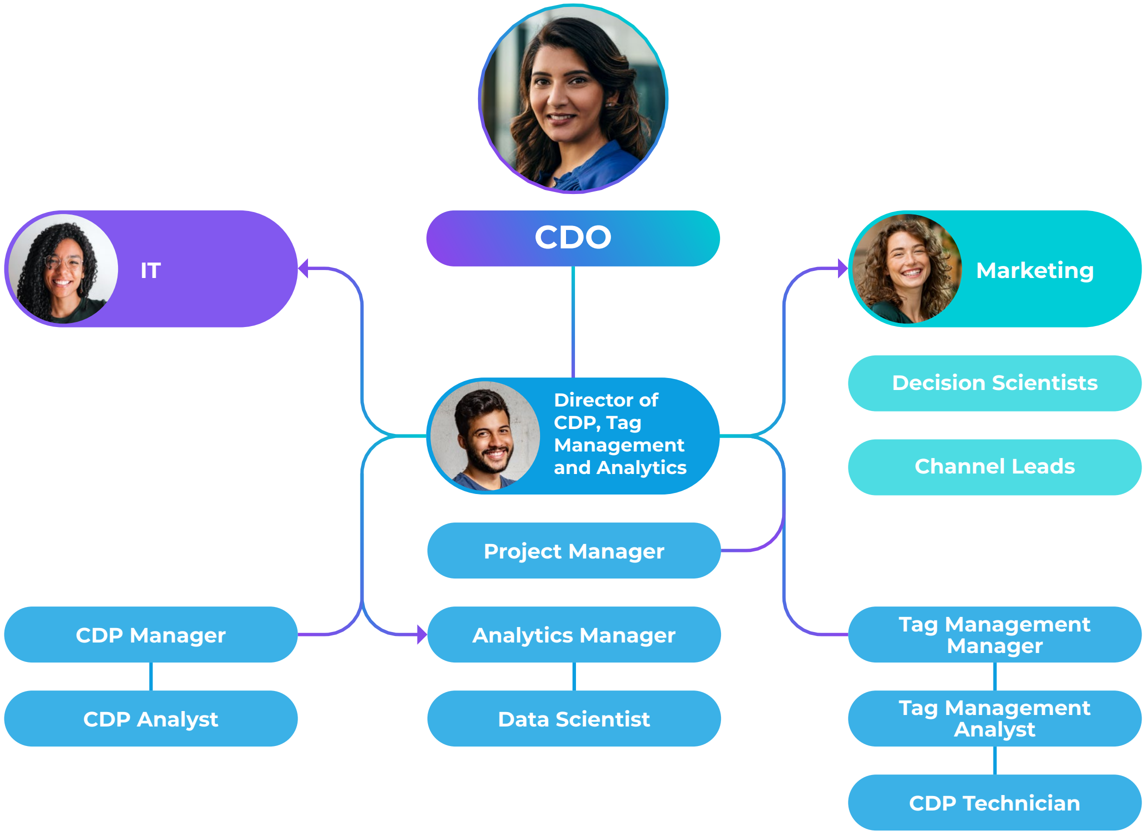
Personalization

Visual Merchandising

Inventory Management

The Data Center of Excellence (DCoE) is a centralized department that specializes in the strategy, design, staffing, and delivery of a Service(s) that the organization requires at scale. The team helps streamline access to unified customer data to increase the speed at which cross-departmental teams can act. They are responsible for defining and answering critical, company wide questions. For example, how to create a data layer that standardizes naming conventions and governance, how to integrate the data infrastructure, how to maintain data security and compliance, and then design a solution and delivery model that helps build out use cases for the data across the entire organization. The Data Center of Excellence will restructure your organization by introducing a new team that collaborates across multiple departments for the purpose of ingesting, organizing, and activating customer data in all ways possible.

Highly Regulated Organizations



Companies in highly regulated industries such as healthcare and financial services have an added layer of complexity when organizing their CDP teams due to the types of data they work with and regulations. Data governance and privacy compliance teams need to be included at a very early stage for every use case, and then in an ongoing and regular cadence, to ensure proper compliance with global laws and standards. While it can seem daunting, highly regulated industries are also seeing some of the most significant benefits from implementing CDPs.

Three Key Recommendations for Establishing Customer Trust Through Data

Recommendation 1: Make Privacy Purposeful

> *“One of the aspects of data governance compliance is knowing what data is being processed, where the data is being processed, and who has access to the data. Having good data governance plays a critical role in achieving privacy compliance.”*
>
> *– DJ Landreneau*
> *Director of Data Privacy Strategy at Tealium*
> *(Page 36, Organization of the Future)*

The first step towards creating a trusted dynamic with your customers is to only collect necessary data and in a way that respects customer privacy. To achieve this foundational goal you will need to:

Create a Great Data Governance Program

Redefine what privacy means to your organization.
Companies need to adjust internal mindsets around data privacy and literally bake respect for customer data privacy compliance into the core of their brand. Almost every employee in an organization will interact with customer data in some capacity so it is critical they understand what privacy means in explicit, clear terms that are then broadcast regularly and visibly. You must also define which individuals own data privacy and establish them as internal Subject Matter Experts (SMEs) for those with questions. Make sure it’s known that data privacy matters.

Draft a privacy manifesto - and make it public knowledge.
Customer data privacy policies for your organization can’t just be spoken, they must be memorialized for the benefit of your employees and your customers! Most customers find brands’ data security notifications extremely complex. **In the US, only 3% of Americans say they understand how current online privacy laws actually work.** Pair that with the **79% of Americans who are not confident companies will admit to misusing their data**, and you can see the trust gap clear as day. Your privacy policies must be clearly defined and properly accessible on your website and internal documentation so that everyone has access to it.

3%

of Americans say they understand how current online privacy laws actually work.

91%

of Americans who are not confident companies will admit to misusing their data.

Prioritize data privacy compliance — for both now and in the future.

Given the global nature of privacy regulations and international business, if you haven't started addressing policies like GDPR and CCPA, to name only a few, you need to start now. Not only is your company required to communicate with and handle your European customers' data in line with GDPR's policies, but making moves to comply now will set you up for success with other inevitable privacy regulations.

Carefully review all data privacy guidelines that apply to your organization and map out your action plan to comply now and in the future. You will need to build in flexibility and scalability, as well as make plans to regularly review the laws that govern your compliance around the world and update them as needed.

Use common sense to prepare for the ongoing evolution of data privacy regulations.

When preparing your company for upcoming data regulations, think about the protections you would want for your own data.

Key steps include:

- Create a data map that clearly spells out the data your company has, what you're doing with it, and where it's going
- Clearly define your current position around data sales and future plans for use of Third Party data
- Insert mechanisms to deal with data access, modification, and deletion based on individual rights

Remember that trust is a company-wide effort.

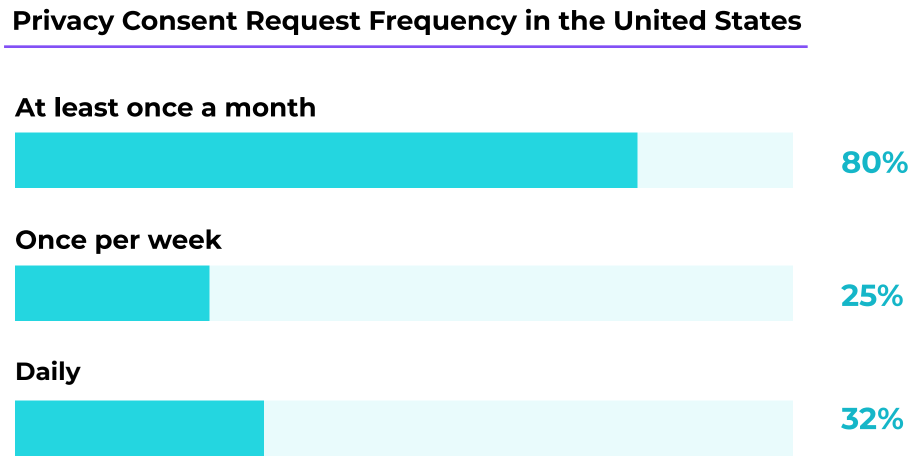
As we mentioned above, your company should incorporate your data privacy stance into its mission statement and core company values. All employees in your organization who touch customer data should understand and be concerned about data privacy. They will rally around this prominent effort to put respect for customer data first. It will help your own team become your primary brand advocates by establishing an internal foundation of confidence and conviction, which will then resonate outward to help build trust with your customers.

Recommendation 2: Give Customers a Reason to Opt-In

Customers are tired of being asked for permission and the fatigue from being constantly asked to provide privacy preferences when visiting websites is real. According to Pew Research, **80% of American adults claim they get asked to agree to a privacy policy at least once a month**. Another **25% claim that this happens almost daily**. Of Americans who get the privacy agreement, **32% say they see one around once per week**.

With all these consent requests coming at your customers from all corners of the internet, you must be really strategic about how you are asking for consent. Consent should be approached as an ongoing relationship with your customers that includes an opt-in request and a value exchange strategy that keeps the customer coming back for more instead of taking their data and running. This is also why marketers can't just leave this to the privacy, data, and IT departments.

How you collect your customer data is as important as what data you're asking for.



Design Your Ongoing Data Collection Strategy

Be transparent about your transparency.
Your privacy policy doesn't just apply to your most well-read, tech-savvy customers. Customers are starving for companies to explain their practices in concise, straightforward language. Doing so will bolster your company's reputation as trustworthy — the clearer your policies, the less it appears you're hiding something. Don't gloss over the realities of how you'll use the data or try to trick customers into providing information. Complicated legalese is not only a turnoff, it's a turn-away. Keep it simple, keep it clear, keep it honest..

Design a Value Exchange where and when it matters.

> *Thinking about how we're going to segment our customers requires us to gather data on them and the key for that is to build trust, have a strong value exchange, and understand that the common consumer today knows that nothing is free. If you're filling out a form, you're giving some data and you expect something in return, so it's on us to make sure that value exchange is clear and also that we deliver on what we say we're going to do."*
>
> ***– Jetta Hansen***
> *Senior Data Analyst at Nav Inc.*

Rather than keeping data collection in the background, turn it into a handshake with your customers. When people arrive at your digital properties, it's important to treat it as the first step in a mutually beneficial relationship. A privacy banner with appealing aesthetics and clear language will be your brand's first impression and should communicate the importance that your company places on the currency of data. And it shouldn't stop there, the Value Exchange should continue beyond the First Party data and PII. Zero Party data exchanges where your brand asks a customer for their opinions and insights in the form of surveys and feedback should happen at the moment in a journey where it makes sense. This brings the Value Exchange into a continuous greeting between the customer and your business, where the relationship can deepen and expand over time.

Turn your request for data into a CX of its own.

It's an exercise in honesty that shores up customers' trust in your brand and helps explain why you need their data. The savviest organizations turn the data collection experience into a critical point in the value exchange. Tell your customers explicitly how you will use the data you're requesting to constantly improve individualized experiences, with specific examples based on your own offerings. Do you sell clothes? Let them know you'll use their data to give them discounts on their favorite jeans. Make the data exchange experience exciting!

Make data access crystal clear.

Enabling your customers to have control over the data you collected will foster a trusted relationship. This would include allowing your customers to access their personal data, correct their data, have their data deleted, or take it to another provider. This should not only be possible, but easily done. The added benefit here is that if your customers are maintaining their own data, your data quality will improve, which in turn makes your personalization efforts more successful. In order to empower your customers to manage their own data, you need the right technology in your stack to do this at scale, across all channels in a cohesive way, and in real-time.

Bake in future flexibility.

The type of data companies can collect is evolving on a constant basis and it's impossible to guess what your company's policy will need to include in five years. Allow room for changes to be made that reflect politics, customer demand, and new technologies. Also, apply a universal approach to the way you handle your entire company's data set. While a pop-up window is an option for today, it could be banned a few years down the road, or all your forms may eventually require double opt-in. Consider all possibilities when building out systems and investing in technologies that help you collect and manage customer data.

Applying strict, clear language around consent requirements, access rights, and security protections will go a long way toward eliminating confusion, both internally and with your customers.

Bonus tip

Keep it consistent.

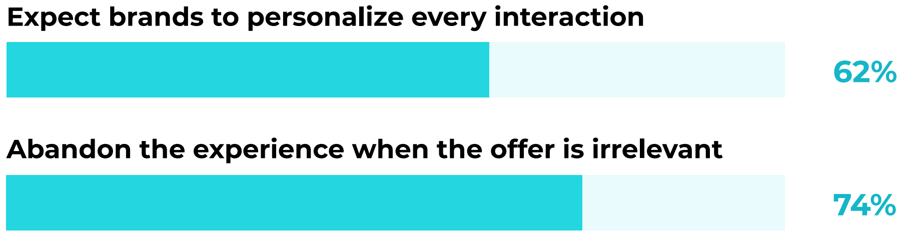
Recommendation 3: Map Out a Customer Journey That Builds Trust

Customers now require a relevant experience, which depends upon unified customer data. When you have unified customer data, you're able to present your organization in a cohesive and meaningful way to your customers. When data isn't unified, it becomes painfully obvious. Whether you're running digital ads promoting products your customer already purchased or sending emails after an unsubscribe or opt-out request, customers know when your teams aren't working in concert because it leads to bad customer experiences. But instead of seeing this as a harrowing challenge to overcome, see it for what it really is - an opportunity to create amazing trusted experiences.

With the right Martech stack (that maximizes your customer data in a privacy-compliant and flexible way) you can create amazing customer experiences and brand loyalty. You've determined what data you absolutely need to collect to optimize your business operations. You've created a winning strategy for collecting the data, communicating how it will be used and how to access it. Now you have to segment and activate the data!

62% of customers expect brands to personalize every interaction and 74% said they feel frustrated enough to abandon the experience when the offer is irrelevant to them. By mapping out your customer's unique and personalized journeys, you can obtain a better understanding of your customers and deliver one-to-one marketing communications that are also scalable.

Privacy agreement Online Data & Internet Privacy in United States



Create and Deliver a Personalized Customer Journey

Define your customer audiences and segments respecting consent preferences.

Personalization can be done at scale with the help of a solution such as a CDP. You will be able to define very targeted audiences as starting points for outstanding customer journey maps. Have your CDP built out with these key audiences and assign your customers to these audiences while respecting your customer consent preferences.

Plan out meaningful touch points and build in marketing automation.

Once you have your starting point (when the customer enters into an audience), define where you want to take them and what content, messaging, special offers, and value you will provide along the way to drive them to the ultimate destination based on their consent.

Be transparent on how you're using their personal data throughout their experience.

Similar to letting people know how you will use their data when you initially collect data from a customer, you will want to maintain this transparency throughout the customer journey. It may seem obvious once you've received permission to use their personal data, but customers need to be constantly reminded that you're working for their benefit!

Make sure to provide off-ramps for customers in their customer journey.

t's possible that a customer will get placed into a journey that they will quickly discover doesn't suit them. Maybe something in their external world has shifted (perhaps they have moved and their daily needs have shifted), or perhaps something that was originally appealing, isn't so awesome anymore. Don't make it hard for these individuals to leave a journey. And definitely don't make the only option to "unsubscribe." When they change their mind, make it a learning experience for both of you.

Include customer access to data controls in every channel.

On that note, make it easy and even empowering for a customer to determine their own interests and update their own data. Offer this access through every touchpoint, as possible, and use a Martech stack that is flexible enough to manage this functionality. Your customers will appreciate the simplicity and empowerment. Turn it into a way to build trust and deepen customer loyalty instead of turning customers away.

Keep your messaging and language consistent throughout.

Along with providing access to data controls in every channel, make sure you're using consistent language and messaging around your privacy policies so it's easily recognizable and understood. Consistency is a major component of a strong customer experience and consistency in privacy messaging will only grow in significance as time goes on.

Build in enough flexibility to address the shifting privacy landscape.

Privacy regulations are constantly evolving with the focus on protecting consumers and empowering them to control their data. With that being said, companies need to adapt quickly as these regulations shift, and to do that, they need to put into place the processes and infrastructure to be prepared for now and in the future. Companies that are not prepared will be forced to rework their entire infrastructure and strategies and be at risk of becoming laggards. Therefore, it is important to engage with your data privacy professionals when mapping customer journeys and focus on continuous optimizations.

An excellent example of preparing for the future is the investment in a First Party data approach. We all understand that the demise of Third Party cookies is on the horizon and so progressive companies are embracing trusted First Party data strategies enabled by a CDP.

Avoid competing journeys for your customers.

One pivotal component of respecting your customer's privacy is to not overwhelm them with unnecessary engagement. Avoid putting customers into too many or competing journeys. You will need to prioritize the customer journeys and rely on AI and Machine Learning, like Tealium Predict ML, to serve the right message at the right time. ML techniques have been proven to not only comply with privacy laws, but also deliver a new revenue stream that both consumers and businesses will benefit from.

Why Companies Around the World Trust Tealium

> ***"Consent management is essential to the organization of the future. With Tealium, Kmart has consolidated company-wide consent streams to deliver privacy-first customer experiences at every touchpoint. We believe this approach has future-proofed our business to remain compliant in an evolving regulatory landscape."***
>
> ***– Photi Orfanidis,***
> *Architect, Marketing & Loyalty*
> *Technologies at Kmart Group Australia*
>
> ***"With Tealium, we can make the most of the data our clients share with us. By using First Party data with our customers' consent to build a 360-view, we can improve engagement by delivering more useful, personalized content while prioritizing their data privacy. This allows us to be there for them during the moments that matter most, whether they're reporting a lost card or planning to buy a house."***
>
> ***– Bobby van Groningen,***
> *IT Engineering Lead at ABN AMRO*

Tealium founded the Customer Data Platform space. Our journey began when our founders, Mike Anderson and Ali Benham, created the tracking pixel at WebSideStory (now Adobe Systems) and invented the tracking of customer behavior online. Tealium created the first CDP in 2013 and has worked with over 1,000 enterprise companies and highly regulated industries.

Tealium offers a full suite of services for the management of customer data in real-time, across all channels and devices, with over 1,300 integrations, data centers around the world, and privacy compliance baked into our DNA. We are a data-first CDP, and privacy and consent were not an afterthought but a driver toward using customer data to create the ultimate customer experience in a trusted manner. The privacy and consent landscape is shifting rapidly and continuously. Organizations are being tasked with adjusting in a way that's flexible enough to provide effective CX while continuing to comply with new regulations and changes in technology. To achieve this complex ambition, companies need a unifying solution integrated throughout the tech stack, so that automated enforcement of privacy can occur in harmony with the experience.

Addressing evolving privacy and consent requirements in today's competitive landscape means that we must rely upon automated governance of data taking place at the same time the CX is being orchestrated. This means that this central solution must serve as a trusted repository of customer data for the enterprise to deliver on the promise of end-to-end privacy compliance.

Some features the central solution technology should include:

- Tag management to streamline data collection on websites
- Integration with CMPs that manage privacy inventory and Data Subject Access Requests
- Central data management functionality that is automated
- Dashboards for visualizing the data supply chain throughout all journeys
- InfoSec certifications to validate their commitment and adherence to privacy regulations
- Identity resolution in real-time to ensure preferences are applied accurately prior to activation
- Broad integration with all other customer-facing technologies that incorporate the same privacy principles and deliver in real-time

This is best achieved in a unified, real-time Customer Data Platform, extensible with CMPs, and capable of deep integration with customer-facing technology channels and analytics solutions.

Enter Tealium.

Tealium's Role in a Privacy and Consent Initiative

Tealium's first role in a privacy and consent initiative is to **act as the governing platform tasked with the collection of the customer data** it is configured to work within an automated fashion.

When it comes to managing customer data privacy, Tealium's Customer Data Platform plays a central role across the entire data supply chain. First, Tealium's data collection technologies collect customer data sets alongside their privacy preferences, in real-time, on any type of device.

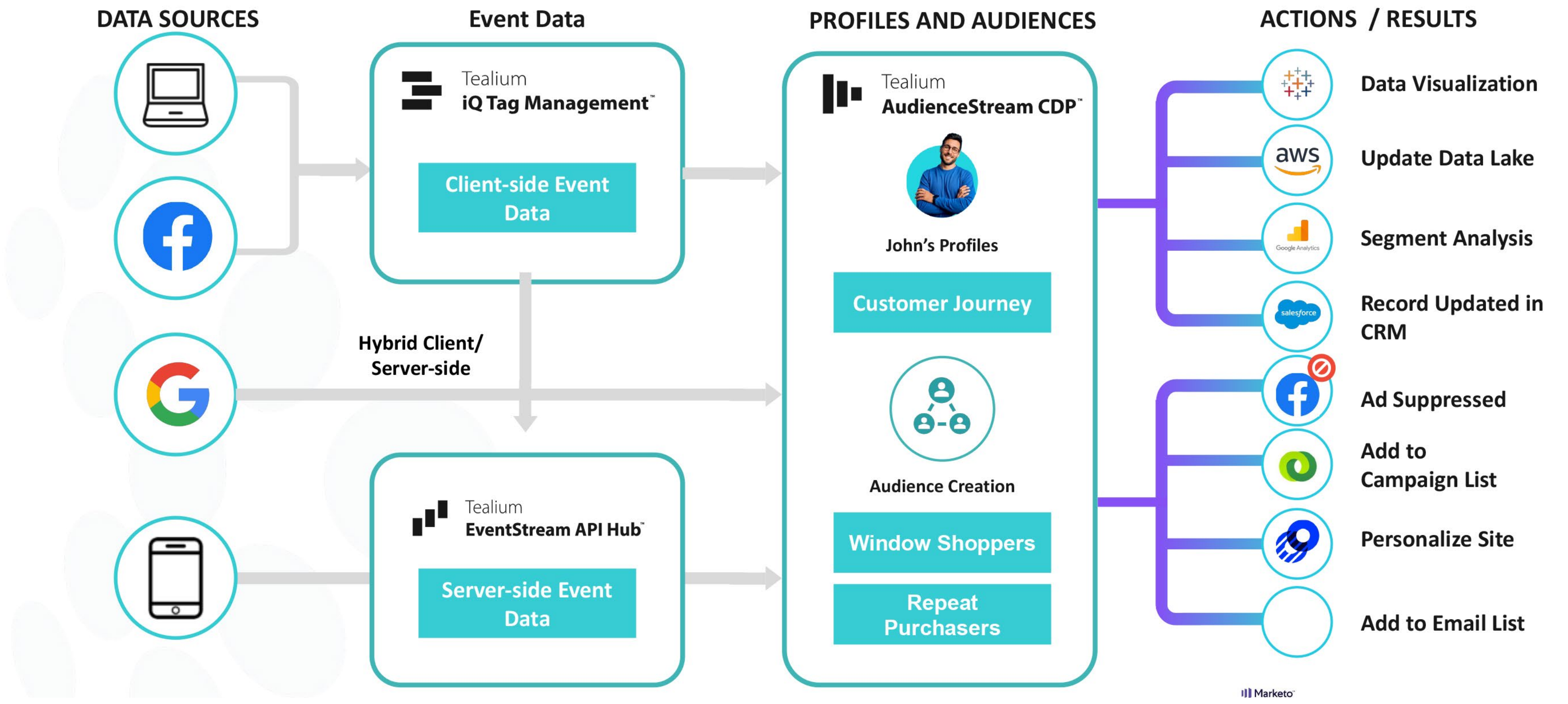
Privacy preferences can be collected:

- through the built-in Tealium Consent Manager banner (the form factor and specific Privacy Regulation to be determined by the business)
- through another external technology of the business's choice
- in some cases, companies may not offer a pop-up banner and instead a designated "Privacy Policy" web page configured to represent these preferences

In any of the above scenarios, Tealium detects those customer preferences and enforces them while also collecting other pertinent data that applies to the customer, such as demographic, navigational, and transactional datasets. Finally, based on the preferences of the visitor, all data is orchestrated and routed by Tealium to the appropriate technology destinations.

Tealium backs its security and privacy options with Third Party certifications including HIPAA, ISO 27001 & 27018, Privacy Shield, and SSAE18 SOC 2 Type I & II. We can help you meet whatever privacy regulations your policy or industry requires.

Consent Acquisition



Tealium iQ (TiQ) Tag Management

The Tealium iQ (TiQ) Tag Management System for websites has the ability to detect, collect, and transmit customer data as they emerge in real-time, including opt-out/opt-In decisions and categorical preferences of marketing.

Tealium EventStream API Hub

Tealium EventStream collects data on websites, mobile Apps, IoT, and OTT devices that can be routed to the Customer Data Hub and the CDP for additional reconciliation with a unified profile. In addition, Tealium provides programmatic and file-based interfaces for the same purposes.

Consent Management & Orchestration

After acquiring Consent, Tealium's second role is to **orchestrate the enrichment and activation of that data throughout the technology ecosystem**.

Once a customer has provided consent, the business may establish a customer profile that reflects their chosen experience and engagement needs. This surfaces many more requirements to maintain customer data integrity and portability.

Tealium's solution set expands into managing the lifecycle of consent within the AudienceStream CDP for this purpose.

Tealium AudienceStream CDP

Data Collection is not a one-time task. Customer preferences are always evolving, causing changes to the Customer Profile as a result. Tealium AudienceStream CDP integrates directly with TiQ and EventStream to reconcile the changes in data and associated identity as ongoing user sessions are captured on websites and other devices. This type of automation directly addresses cost, time, and risk otherwise associated with manual data privacy management or on a silo-by-silo basis. AudienceStream governs the precise changes to customer data and automates the evolution of the dataset over time. This evolution leads to producing new behavioral insights on the customer and is appended to the dataset immediately.

Tealium's CDP governs which technologies receive customer datasets, and even more importantly, which ones can orchestrate precisely the necessary amount of data.This ensures that customer data is being used on a "need to know" basis. In addition, Tealium's CDP has built-in security features that allow for data to be designated as Personal Information (PI) as required by every privacy regulation and can be configured to treat that data securely and according to law. This includes encryption techniques, hashing techniques, de-identification techniques, and restricted storage capabilities.

Tealium Partner Integrations

The orchestration of the customer profile will involve purposeful and compliant orchestration of customer data with the entire technology stack in the business. Tealium integrates with over 1,300 technologies using an intuitive interface to add value in this effort. Not only are the destinations of the customer data effectively orchestrated in this manner, but also the sources upon which the data is surfacing are included in the automation. Various other online and offline customer touchpoints produce relevant customer data, and Tealium's platform is configured to connect to each of them as required, mitigating the risk that custom engineering would present to a rapidly evolving business strategy.

Engineered for Scale and Reliability

Customer data is one of the most valuable assets for any enterprise company. Even a tiny blip in uptime can create problems in compliance and personalization when that data is delayed or lost. Make sure your CDP vendor can meet your global and regional data center needs and has a proven track record of reliability and availability.

While downtime is a big concern, one area that doesn't get discussed enough for foundational technologies like a CDP is the pain and costs associated with ripping it out and replacing it. Choosing a data-first CDP that can scale and grow with your business through the flexibility of vendor neutrality ensures your investment into your customer data won't need replacing as you expand into new geographies or increase how much data you're processing.

Developed for Enterprises, Built for Everyone

Tealium is trusted by the most demanding enterprise customers, nearly 1,000 global enterprise level customers across numerous industries - including retail, healthcare, pharma, sports and entertainment, travel and hospitality, gaming, insurance, government, education, automotive, and many more. These companies trust Tealium not only for our enterprise grade security and permissions but also for our platform's speed and reliability.

Contributors

Julian Llorente Perdigones
DJ Landreneau
Ted Sfikas
Matthew Parisi
Phil Hollrah
Karen Naves
Heidi Bullock
Hilary Noonan

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