freshworks

# GDPR and CCPA Compliance with Freshworks

# Table of Contents

# Overview

According to **Forbes**, regulatory compliance is not only essential for organizations to save costs but is also critical to maintaining a healthy reputation. In 2018, the **average cost** for organizations that experienced non-compliance problems was around $14.82 million, a 45% increase from 2011. These ever-increasing financial and reputational costs of non-compliance can only be minimized if your technology vendor understands your compliance-related concerns and follows necessary protocols to ensure privacy and security, every step of the way.

If we look closely at the Customer Engagement and IT functions today, they require a fair bit of monitoring in order to stay compliant with local and global regulatory requirements while maintaining great customer and employee experiences.

CX and CRM teams constantly deal with large quantities of customer data while interacting with them on a daily basis. This data sits in silos and needs to be thoroughly combed and analyzed not only to derive actionable insights but also to ensure regulatory compliance. Businesses need to ascertain no personal data is used without consent or out of regulatory norms at any point in the non-linear customer journeys of today's digitally-driven business-customer engagements.

IT systems, on the other hand, use large quantities of data through several security-related areas they are responsible for and hence are at great risk of data breaches and breaking regulatory norms. IT systems of today need to stringently follow best practices across teams to ensure tight regulatory compliance and data security.

While GDPR secures the data privacy rights of people in the European Union, CCPA regulates privacy and consumer protection related norms in California, USA. It is increasingly becoming a mandate for businesses to comply with all the regional and global regulatory requirements. They need technology vendors who are reliable when it comes to user data protection and security.

Read this paper to know how Freshworks follows industry best practices and ensures conformance to GDPR and CCPA in order to maintain the privacy and security of its customers' data.

02

# Industry drivers of compliance requirements

## Compliance and Customer Engagement

Regulatory compliance plays a pivotal role in customer-facing functions. Whether it's Customer Service, Sales, or Marketing teams, they all work with large amounts of customer data on a regular support. While this data is always important to create moments of delight for the end customer, the way this data is used is always under scrutiny by regulatory bodies.

Let us dig deeper into what compliance means from the Customer Experience and Customer Relationship Management perspectives.

## Customer Experience

Customer Support, Sales, and Marketing teams work with large amounts of customer data on regular basis. The way this data is used is always under scrutiny by the regulatory bodies.

Regulatory compliance may come in the way of delivering a great customer experience. Customer experience can often be adversely affected by time-consuming compliance processes. Striking the right balance between regulatory compliance and customer experience, therefore, becomes a business necessity.

There are several drivers that further complicate the CX function's adherence to compliance

**1. Multiple channels and touchpoints**

While omnichannel experience has now become the quintessential part of the customer experience function, it has made it increasingly difficult to unify customer data across touchpoints in a compliant way.

**2. Siloed customer outreach**

Multiple teams communicating with the same set of customers can be detrimental to both CX and regulatory compliance. For example, executing multiple marketing campaigns to the same audience across channels without taking their consent for all kinds of communications may neither be a compliant way to reach out to customers nor a pleasant experience for them.

**3. Business expansion and scaling**

Scaling across functions and geographies may often fall under the purview of new regulations. As businesses scale, offering a consistent customer experience is a challenge and the compelling need to fulfill new regulatory requirements may lead to more complicated customer onboarding processes, delayed responses to matters that need immediate attention, and dissatisfactory experiences in general through the customer relationship lifecycle.

This essentially means compliance needs to be the common building block of every CX effort. To ensure that, businesses need to choose their technology vendors carefully.

Key considerations to implement CX solutions for your business

- Use a CX suite with an embedded compliance framework
- Ensure local compliance requirements are met in every geography you operate in but customer experience is maintained consistently at a global level
- Deliver a unified experience through intelligent insights to ensure tight regulatory compliance.

A modern, data-driven, and intelligent CX function, therefore, is the prerequisite for both compliant systems and great customer experience.

## Customer Relationship Management

CRM systems use a whole lot of personal data and this means they are closely associated with consent management. They are also among the most exposed systems to data breaches since they use several channels such as email, messaging, telephony, and website forms. This makes them the most susceptible to hacks, access rights breaches, and other kinds of security attacks.

Businesses need to ensure their CRM systems are CRM systems are exposed to data breaches since they use several channels such as email, messaging, telephony, and website forms. They need to follow certain best practices in order to build rock-solid customer relationships in a compliant manner.

### 1. All information available at the fingertips

Customer data from CRM systems can be used to create better synergy between functions, streamline marketing efforts, and ultimately sell more in a customer-centric way.

One of the most important goals of a CRM system is to is always to provide data when and where it's needed the most- across business units. But if this data does not fulfill regulatory requirements, it could lead to serious repercussions in terms of time, money, and image.

Businesses need to ensure their CRM systems follow all local and global compliance requirements and can provide them insights into their customer relationship lifecycles- right when they need it.

## 2. Stringent control processes in place

With the ever-changing regulatory landscape, businesses need their CRM systems to have transparency around how they use customer data. They also need to have mechanisms for on-demand erasure and management of all privacy-related requests centrally and seamlessly.

## 3.Consent management

In today's tightly regulated world, CRM systems closely need to follow consent management principles. Acquiring, storing, and regularly updating user consent across channels becomes the key to ensuring a privacy-safe environment and healthy customer relationship management.

## 4. Subscription management

According to GDPR, even when a contact has given consent to receive marketing campaigns and communications from your company, they should always have the right to object or opt-out from receiving marketing communications in the future. Email marketing specifically falls into the purview of regulatory requirements related to subscriptions and businesses need to

- Obtain re-permission from legacy contacts
- Obtain new permissions for marketing communications
- Manage automation

Not only this, but businesses across industries also need to ensure they have mechanisms to give back the right to user data to the users when they ask for it. This requires keeping a record of all opt-outs and regularly updating them and making regular checks to ensure they are not part of any customer communication.

# Compliance and IT

The role of IT as a function in maintaining compliance becomes important in technology-dependent areas such as information security and privacy.

According to Gartner, “IT risks have been managed in silos, but are increasingly being recognized as leading indicators for failure in other risk areas, such as fraud, and resiliency.”

IT systems of today handle a multitude of areas such as identity management, audit logs and authentication, change management, trouble ticket tracking, risk assessment, and disaster recovery. For large and mid-sized organizations, all the aforementioned processes need to be maintained across functions tirelessly while ensuring data and information security. This makes IT systems extremely vulnerable to security attacks, especially given the deluge of data they produce in order to run their everyday business.

The role of IT as a function in maintaining regulatory compliance becomes especially important in technology-dependent areas such as information security and privacy. There are several recommended best practices for IT functions in order to become compliant

- Keep a track of all current tools across business units
- Conduct regular risk assessments to identify gaps
- Plan ways to bridge technology gaps
- Review and optimize according to local and global regulatory parameters

Growing businesses grapple with IT systems that cannot scale enough to meet the long-term needs of compliance. Meeting fast-evolving regulatory needs requires businesses to invest in sophisticated IT systems.

Businesses need to evaluate their IT vendors through thorough planning, assessment, and review. This will help them standardize their processes and abide by all mandatory regulatory norms.

03

# Compliance standards of today

## General Data Protection Regulation(GDPR)

The European Parliament adopted GDPR in April 2016. It carries provisions that require businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. The GDPR also regulates the exportation of personal data outside the EU. Non-compliance could cost companies dearly- up to 4M Euros or 4% of their global annual revenue, whichever is greater.

GDPR provides a framework for businesses to standardize and regularize real-world security and privacy needs of an individual's data used for business purposes.

The key principles which the GDPR requires businesses to operate on revolve around lawful, fair, and transparent processing of user data, purpose limitation, data minimization, accurate and up-to-date processing, limitation of storage in a form that permits identification, confidentiality and security, and accountability and liability of users' personal data.

Naturally, for businesses, GDPR necessitates the implementation of robust data security and privacy frameworks. Businesses need to handle all customer data with utmost care across touchpoints, whether it's marketing efforts, sales reach outs, or new efforts to improve customer experience on different channels.

## GDPR Compliance at Freshworks

All Freshworks products provide GDPR-ready capabilities to help our customers meet their compliance obligations. Freshworks extends these capabilities not only to customers in the EU but to all our customers worldwide.

- Empower- Ensure fair and transparent processing of customer data
- Secure- Incorporate security by design in products, to protect personal data
- Unify- Streamline processes to help customers meet compliance obligations

Committed to protecting our customers' personal data, Freshworks is here to help our customers understand the significance of the GDPR, its requirements, and our allegiance to align with global standards.

**Features built for GDPR readiness**

**1. Right to be Forgotten**

Freshworks products let you delete customer/agent data permanently. You can delete the customer/agent's profile and all the data associated with it like tickets raised by them, team huddle discussions, phone conversations, chats, satisfaction ratings provided, topics created, and discussions in forums.

A delete or an export request from a customer would have to be routed via the admin who validates if the requestor is genuine.

- End-User Profile Deletion- Freshworks products currently support the deletion of end-user profile information with an option of soft delete as well as permanent delete which will erase all associated data like tickets, forums, calls, and so on.

- Agent Profile Deletion- We currently support the deletion of Agent profile information with soft delete and permanent delete options where all their contributions like knowledge base articles, tickets, and team huddle discussions are anonymized and all PII (Personally Identifiable Information) are deleted forever.
- Ticket Deletion- Freshworks customers can delete tickets. In doing so, all team huddle discussions associated with the ticket are deleted along with it.
- Attachment and Image Deletion- Customers can delete attachments and images by deleting the support tickets to which those attachments and images are attached.

In addition, Freshworks customers can leverage APIs to assist with their GDPR compliance efforts in a secure environment with no access unless explicitly approved by senior management to comply with applicable laws. These archived logs are also purged automatically after 12 months.

**2. Right to portability**

Freshworks products support export requests from customers. A customer can export user contact details, tickets of the user, forums the user has contributed to with the respective APIs.

An export request from a customer would have to be routed via the admin who validates if the requestor is genuine. Customers can leverage the following APIs to assist with their GDPR compliance efforts on data portability:

- User Profiles can be accessed using View a Contact API. Customers may want to only export fields visible to the customer using the 'displayed_for_customers' property of the API.
- Tickets of the User- Users can list tickets by requester using List Tickets API. They can also access conversations by Ticket Id.
- Forum contributions- user contributions to forums can be accessed using APIs.
- Satisfaction ratings provided by users can also be accessed using APIs.

**3. Right to Rectification**

The GDPR includes the right for individuals to have inaccurate personal data rectified or completed if it is incomplete. End-users and agents in Freshworks products can rectify any errors in their personal data by editing their profiles.

# The California Consumer Privacy Act (CCPA)

CCPA became effective on January 1, 2020, and is meant to enhance privacy rights and consumer protection for residents of California, United States. CCPA allows users to get their personal information prohibited to be sold to other companies. It also provides users with complete control of their data with an option to ask companies to anonymize their data or opt-out of data collection platforms, if they want to.

Since CCPA gives users the right to ask for information about how their data is being consumed, businesses need to be wary of the way they collect, keep, and use customer data. This requires clear visibility of customer data across functions and secure frameworks to not only process it but also remove it when customers ask to delete or opt-out.

## CCPA Compliance at Freshworks

Subject to the provisions of the CCPA, Freshworks customers have the right to request the following:

1. **Right to request information about the:**
    - Categories of personal data under which Freshworks has collected information about them.
    - Specific pieces of personal data Freshworks has collected about them
    - Categories of sources from which the personal data is collected
    - Business or commercial purpose for collecting personal data
    - Categories of third parties with whom the business shares personal data

2. **Right to request for deletion of any personal data collected about customers by Freshworks.** If customers want to exercise the foregoing rights to access or delete personal data that constitutes 'personal information' as defined in CCPA, they can contact Freshworks to initiate that process.

The list of categories of personal data collected and disclosed about consumers and the list of categories of third parties to whom the personal data was or may be disclosed are available on our website. Separately, Freshworks does not sell customers' personal data.

04

# How the Freshworks Neo platform enables compliance and enterprise readiness

Over 40,000 customers across the globe trust Freshworks with their data security. We back ourselves up with robust data security and privacy practices that form an integral part of our product engineering and service delivery principles.

Following the tenets of security by design and privacy by design, security and compliance are at the heart of how we build our products, secure customer data, and provide high resiliency. We have top-down governance and security in our DNA that lets us constantly wade through our threat vectors and calibrate to strengthen our security posture. That way, we align with the changing business and technology landscape.

In order to make customer data impeccably secure and stay compliant with all local and global regulatory requirements, we follow a multi-tiered data security model and maintain end-to-end security in the product life cycle. We employ a resilient architecture that is backed by the Freshworks Neo platform- an end-to-end and highly flexible platform that is designed to unify customer experiences, enhance employee productivity, and empower an ecosystem of developers and partners while maintaining world-class security and regulatory compliance.

Here is how Neo infuses security controls into our product suite and helps our customers stay compliant.

> Freshworks employs a resilient architecture that is backed by the Freshworks Neo platform. Neo is an end-to-end, highly flexible platform that is designed to unify customer experiences, enhance employee productivity, and empower an ecosystem of developers and partners while maintaining world-class security and regulatory compliance.

## 1. Security in the development phase

**Secure Coding** - Security at Freshworks starts in the engineer's IDE. Various standardized tools are run as code is typed out, providing instant and continuous feedback to engineers. Engineers also undergo InfoSec training to understand secure coding practices sessions and the dangers of various security and compliance vulnerabilities introduced by certain types of programming practices.

**SAST and DAST** - In our Continuous Integration systems, Static Application Security Tests (SAST) and Dynamic Application Security Tests (DAST) suites look for potential vulnerabilities. Our in-house Deployment Engineering system, Freshworks Cloud Platform (FCP) is designed to reject applications that do not pass these tests, ensuring Freshworks products are always built-in a secure environment while maintaining regulatory compliance.

**Container Scanning** - This is the third and final line of defense before a code can run in any of our environments. We use AWS's Elastic Container Registry (ECR) where we subject all containers to security scans. Within a container, both Freshworks code and all open-source libraries and other components are subject to security tests.

## 2. Runtime Security

**FCP(Freshworks Cloud Platform)** uses various tools such as Open Policy Agent and Gatekeeper to keep a check on vulnerabilities and secure workloads at various levels. We ensure container images come from the Freshworks repository and only authenticated users are permitted in the deployment environment.

**Workload Protection** - This is the security blanket that is enforced once code is running in production environments. This keeps the asset inventory fully updated in a cloud-native environment and continuously looks for misconfigurations according to various compliances and policies across compute, storage, IAM, etc.

We employ container vulnerability scanning and a Web Application Firewall to avoid malicious attacks. Also, security Information and Event Management (SIEM) is used as a log monitoring mechanism. It follows rules based on patterns and anomalous patterns are identified.

## 3. API gateway for rate limiting and session validation

- The platform employs an API gateway as an integral part of the Foundation Services. This gateway follows a predefined rate and does not allow API calls beyond that limit. This helps the information security team abide by their predetermined security policies centrally.
- Our session validation tool allows the identification of customer agents through session validation. The user is asked to log in again if the session token has expired.

## 4. Spam and virus detection in email

The email service in the Neo platform manages security in all incoming and outgoing emails. This service uses anti-virus detection, anti-spam detection, and email scoring to ensure impeccable security.

## 5. SSO-based validation and session end across products

The platform enables administrators to define and enforce security controls like password policy, two-factor authentication, and single sign-on via the identity provider of their choice and ensure only trusted users gain access to resources. It provides a central view of all accounts and users, helping our customers stay secure.

## 6. IP Rate Limiting

The IP rate limiting service in Neo limits users' sessions (or IP addresses) based on the information in the session cache. This ensures servers are not overloaded and maximizes infrastructure security against threats such as denial-of-service attacks.

This service fronts all traffic that comes to Freshworks systems thereby ensuring information security through a single unified command center to address all rogue attacks.

## 7. Scheduling to delete data

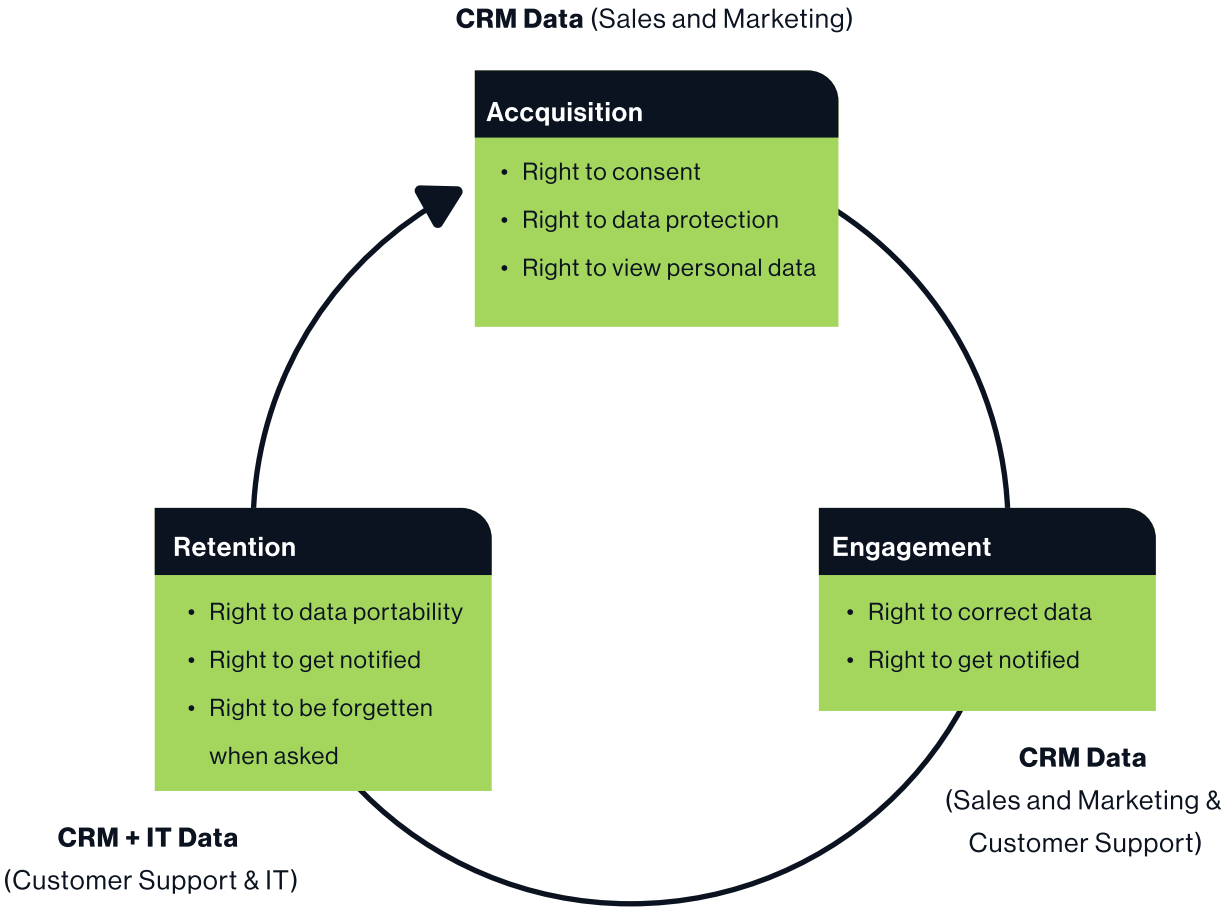
The scheduling service in the Freshworks Neo platform schedules data deletion at regular intervals if the data is not in use, ensuring sensitive customer information does not reside in Freshworks' or our customers' systems unnecessarily. This is a great way to ensure GDPR compliance and data privacy at Freshworks.

05

# Next Steps

Growing organizations today use a huge amount of customer data to run everyday operations and derive actionable intelligence for planning and optimization. Data gets generated and stored through the entire journey with their customers. This means all marketing efforts during the customer acquisition phase, engagement activities post-acquisition, and retention strategies employ large quantities of data that is vulnerable and falls under the scope of regulatory supervision. Even after the customers end their relationship with a business, their data remains with businesses which then needs to be deleted or removed according to regulatory norms.

Acquisition-related efforts are typically aligned to the CRM function and make use of CRM data. Engagement strategies and execution are managed by the Customer Support and CRM functions and use data from the related systems. Similarly, the retention and attrition phases employ support software and applications and make use of data from the Customer Support and IT functions.




Large and mid-sized organizations, due to the sheer scale at which they operate, find it difficult to seamlessly access and use data and insights across functions. The fast-evolving global and local regulatory framework only adds to that complexity if they do not have reliable security frameworks in place. The first recommended step in this direction is to choose a technology vendor that is not only futuristic and data-driven but also keeps data privacy, security, and regulatory compliance at the core of everything it does.


freshworks