ActionIQ

ActionIQ Government Regulations Compliance Brief

Meet data protection and privacy expectations across GDPR, CCPA and more

Table of Contents

Introduction

Prioritizing Data and Privacy Compliance

As the world's become more digitally connected, data privacy has evolved into a top priority for consumers. Regulators have implemented privacy requirements in response, introducing legislation — such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) — that impacts brands across the globe. To navigate the regulatory landscape and build trust with consumers, brands must put data privacy and protection at the center of their business strategies.

This is easier said than done for enterprise companies. Challenges include:

EVOLVING GOVERNMENT REGULATIONS COMPLICATE COMPLIANCE

Beyond GDPR and CCPA — which concern data protection and privacy rules in Europe and California, respectively — proliferating data breaches and consumer demands for greater transparency are contributing to new regulations that emphasize privacy around the world, such as the Brazilian Data Protection Law (LGPD). These laws continue to reshape how companies can collect, use and share data when doing busin-ess internationally.

DATA SPREAD ACROSS SYSTEMS LEADS TO LIMITED VISIBILITY

As enterprises continue to add tools to their technology stacks and collect data across multiple sources, maintaining data governance becomes a struggle. With data scattered across different systems within the organization, data visibility is significantly restricted. This is especially relevant for data privacy practices, as when consumer compliance inquiries come in, it may be difficult to locate source data in a timely manner or fulfill deletion requests.

ActionIQ recognizes the critical role we play in helping our enterprise customers ensure data privacy and support long-term business success. Built with security and privacy in mind, ActionIQ enables enterprises to break down data silos and identify where their customer data lives, all while ensuring compliance with GDPR, CCPA and other regulations related to the storage, use and sharing of personal data. You can count on ActionIQ to be your partner in earning the trust of your customers and staying ahead of the regulatory compliance curve.

In This ActionIQ Compliance Brief, You'll Learn:

- GDPR/CCPA principles and their impact
- How ActionIQ is built with data protection and privacy in mind
- What tools, processes and best practices ActionIQ employs to aid in regulatory compliance

GDPR & CCPA Overview

Enforced since 2018, GDPR set a new standard for data privacy requirements and quickly influenced laws outside the European Union. CCPA, which established personal data rights for California residents, was introduced soon after.

	GENERAL DATA PROTECTION REGULATION (GDPR)	CALIFORNIA CONSUMER PRIVACY ACT (CCPA)
Who is regulated?	**Data controllers** and **data processors** that process personal data regarding EU individuals.	Any for-profit **entity** that does business in California and fulfills a list of monetary conditions, as well as their **service providers**.
Who is protected?	**Data subjects**, defined as identified or identifiable persons to which personal data is related who are EU individuals.	**Consumers** who are California residents.
What information is protected?	Any **personal data** that can be used to identify a data subject. Information linked at the household or device level is not included.	Any **personal information** that identifies, relates to, describes or is capable of being associated with a particular consumer or household, with sozme exceptions.
Anonymous, de-identified, pseudonymous and aggregated data	Pseudonymous data is considered personal data while anonymous data is not.	There is no restriction on a business's ability to collect, use, retain, sell or disclose consumer information that is de-identified or aggregated.

Data Controller & Data Processor Overview

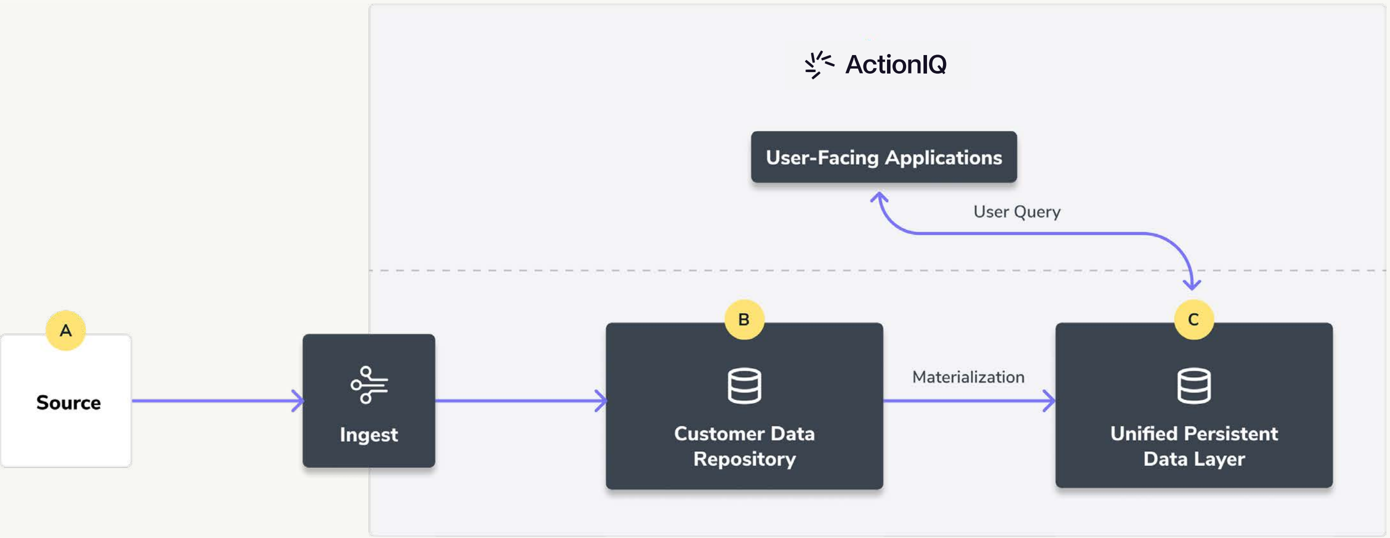
According to GDPR, there are two key roles in data protection and privacy, namely data controllers and data processors. By definition, a data controller dictates how and why data is used by an organization while the data processor processes data provided by the data controller and is bound by their instructions.

	DATA CONTROLLER (ACTIONIQ CUSTOMER)	DATA PROCESSOR (ACTIONIQ)
Who are they?	The authority that controls the procedures and purpose of data usage.	Any individual or party that the data controller allows to use and process data.
What can they do?	• Process collected data using their own processes. • Remain in control of data by specifying how it's used and processed by external parties.	• Process collected data based on the directions given by data controllers. • Not own or control data, or change the purpose and the means by which it's used.
What are their main responsibilities?	• Collect the personal data of customers. • Determine what data to collect, where, how it's used and how long it's kept. • Change or modify collected data.	• Create and implement processes and systems that enable data controllers to gather personal data. • Implement security measures to safeguard personal data. • Store personal data gathered by the data controller and handle the transfer of data to downstream systems.

ActionIQ's Role in GDPR/CCPA Compliance

ActionIQ is a certified, GDPR-compliant **data processor**. Adhering to the concept of privacy by design, ActionIQ's product functionality and robust security measures ensure its data processor responsibilities are met.

ActionIQ Data Storage, Processing and Access



A **Source** refers to the data that ActionIQ receives from clients. An initial snapshot — which is a client's complete data history — will be pushed first to ActionIQ, followed by delta files that contain only the new and updated rows of data.

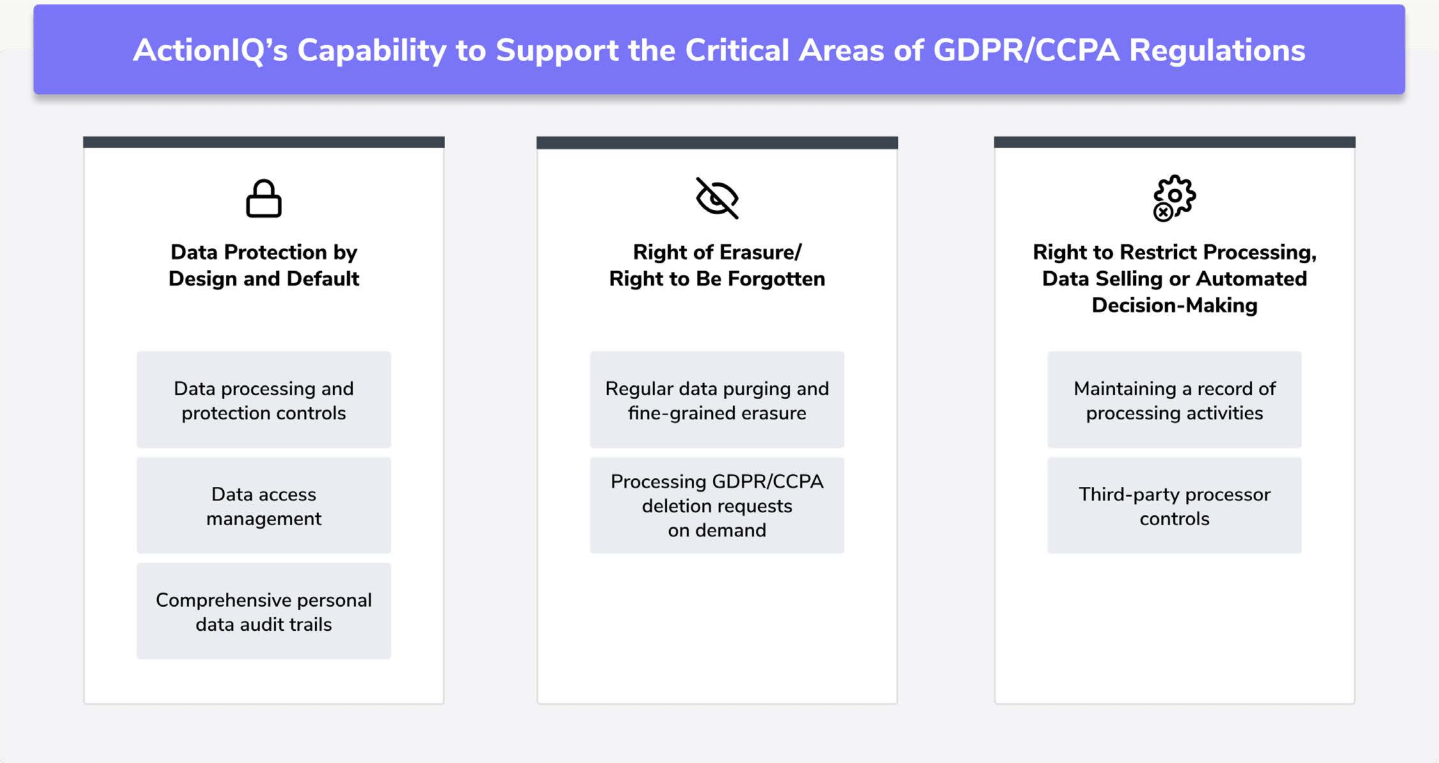
ActionIQ is able to process data containing customer profiles, including personally identifiable information (PII), customer events (e.g., transactions, email events, etc.) and non-customer object descriptions (e.g., stores, products, etc.). When handling data, ActionIQ implements procedures based on the directions given by the enterprises that act as data controllers and is committed to helping them comply with their obligations as indicated by all regulations.

B All batch data ingested will be stored in the **Customer Data Repository**. On a weekly basis ActionIQ will compact the most recent snapshot with all the delta files received until the current time, creating an up-to-date snapshot.

C On a daily basis ActionIQ will materialize the data from the Customer Data Repository into the **Unified Persistent Data Layer**. This materialization creates the tables and data structure that are accessible by users from the platform applications. All user queries are generated on the Unified Persistent Data Layer.

How ActionIQ Ensures Regulatory Compliance as a Data Processor

As a trusted partner to our enterprise customers, ActionIQ designed and implemented the processes and systems needed to meet the mandatory requirements for data processors established by GDPR and CCPA. ActionIQ is ready to support the critical areas outlined by these regulations and fulfill the rights of consumers. Platform capabilities to comply with these regulations include:



ActionIQ's Capability to Support the Critical Areas of GDPR/CCPA Regulations

Data Protection by Design and Default

- Data processing and protection controls
- Data access management
- Comprehensive personal data audit trails

Right of Erasure/ Right to Be Forgotten

- Regular data purging and fine-grained erasure
- Processing GDPR/CCPA deletion requests on demand

Right to Restrict Processing, Data Selling or Automated Decision-Making

- Maintaining a record of processing activities
- Third-party processor controls

According to GDPR, there are two additional obligations for data controllers, namely Right of Access and Right of Data Portability. They are not core requirements that ActionIQ will facilitate as a data processor.

Data Protection by Design and Default

GDPR requires data controllers and data processors to take appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

DATA PROCESSING AND PROTECTION CONTROLS

ActionIQ configures the platform to support single-tenant customer data for each client, providing a high degree of isolation and protection. In addition, encrypted network connections ensure secure data transfer both in and out. Backed by robust security measures, ActionIQ's extended data infrastructure empowers data controllers throughout the entire process, from data collection and storage to analysis and endpoint integration.

DATA ACCESS MANAGEMENT

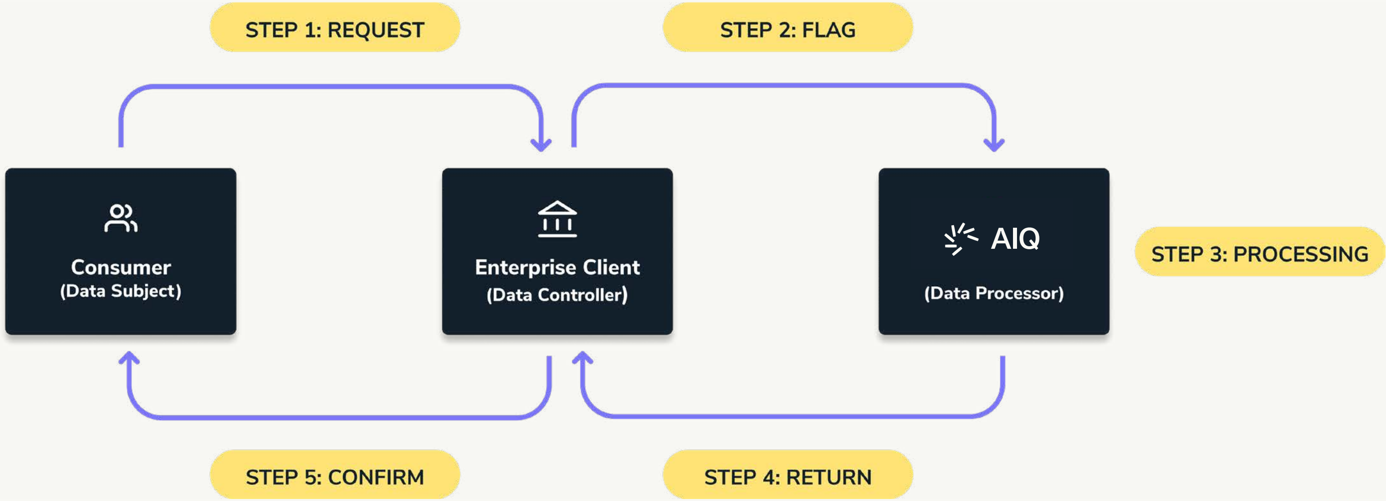
The ActionIQ platform features role-based granular permissions, a self-service portal to manage access and regular user activity tracking and audits to ensure rigorous security controls. A 24/7/365 alerting system is in place to track and flag any attempts at unauthorized access to the platform.

COMPREHENSIVE PERSONAL DATA AUDIT TRAILS

Auditable logs of user activity — as well as data ingest and export events — are available within the ActionIQ administrative tooling. Cloud monitoring and auditing tools are leveraged to provide detailed usage insight.

Right of Erasure/Right to be Forgotten

The right of erasure or the right to be forgotten defines the obligations of a data controller to remove personal data at the request of a data subject without undue delay.



STEP 1 **Request:** Consumer/data subject sends a GDPR/CCPA request.

STEP 2 **Flag:** Client pushes the request to AIQ (through the regular data pipeline), indicating with a flag that a profile must be removed.

STEP 3 **Processing:** AIQ receives the info and fulfills the profile deletion request on the same day.

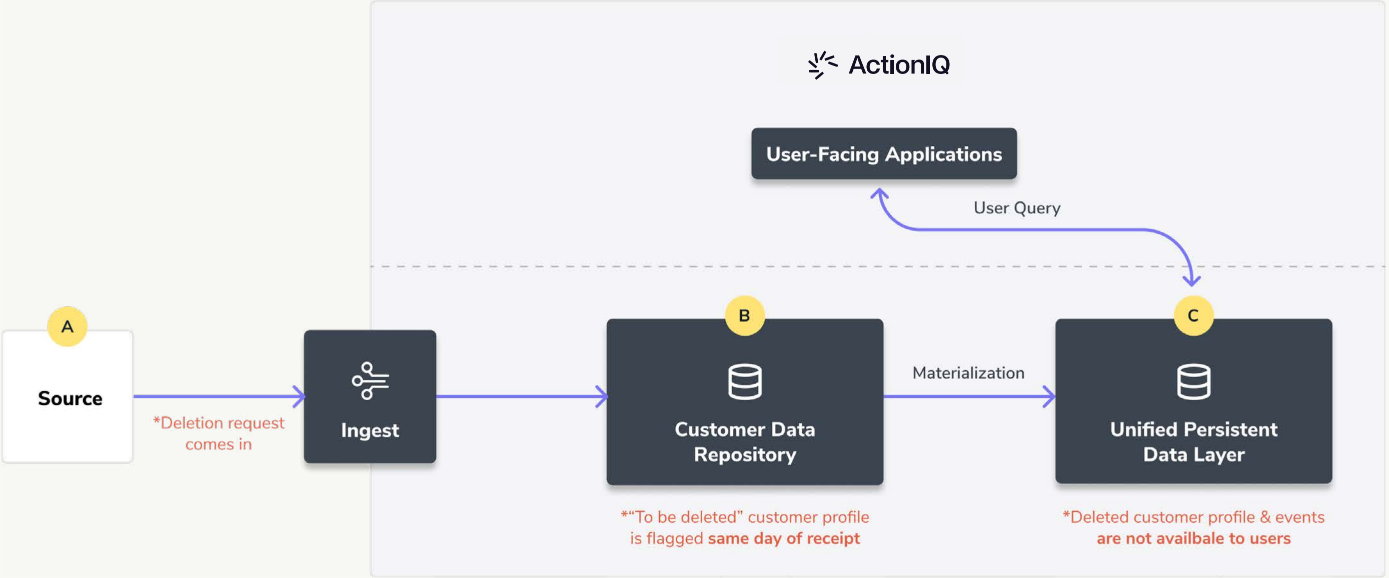
STEP 4 **Return:** AIQ notifies the client that the request has been completed.

STEP 5 **Confirm:** Client sends a confirmation to the consumer/data subject letting them know that the request has been fulfilled.

REGULAR DATA PURGING AND FINE-GRAINED ERASURE

The ActionIQ platform can be used to automatically conduct data purging and fine-grained erasure on a daily basis. Manual removal is also available on demand.

PROCESSING GDPR/CCPA DELETION REQUESTS ON DEMAND


ActionIQ
User-Facing Applications
User Query
A
Source
*Deletion request comes in
Ingest
B
Customer Data Repository
Materialization
C
Unified Persistent Data Layer
*"To be deleted" customer profile is flagged same day of receipt
*Deleted customer profile & events are not availbale to users

- **Same Day of Receipt Removal From Any Query**

  When the ActionIQ platform receives GDPR/CCPA removal requests from the data controller through the regular data ingestion process, the flagged, "to be deleted" customer profiles will be skipped in the materialization process, preventing them from being present in the Unified Persistent Data Layer. This ensures users can no longer access or use these profiles from the day of the removal request.

- **Same Day Removal From Event Tables**

  Any event related to a deleted customer profile is also automatically removed on the same day from the Unified Persistent Data Layer storage. This applies to all tables, including all event tables (e.g., transactions, email events, clickstream, etc.)

- **30-Day Removal From Platform Storage**

  According to GDPR's erasure rule, data controllers have 30 days to provide information on the potential action that's going to be taken on a legitimate erasure request. To comply with the requirement, ActionIQ approaches data deletion via a standardized 30-day cycle. Every week, files that are older than 30 days are deleted from the Customer Data Repository.

Right to Restrict Processing, Data Selling or Automated Decision-making

GDPR and CCPA protect data subjects' right to restrict processing, data selling or automated decision-making for profiling, direct marketing and research purposes.

MAINTAINING A RECORD OF PROCESSING ACTIVITIES

There is an obligation that each processor and, where applicable, their representative shall maintain a record of all categories of processing activities carried out on behalf of a controller. ActionIQ meets this obligation by ensuring this record is captured in our Master Services Agreement with each of our clients. Additionally, we have a functional data map that outlines the type of data we process within our platform and where that data is stored and protected, which can be shared on request.

3RD-PARTY PROCESSOR CONTROLS

ActionIQ works with each client to define and test third-party integrations, including scoping the data being delivered via the integration, prior to launch. Only permissioned users may extract data from ActionIQ and push it to a destination enabled on the platform.

Build Customer Trust While You Boost Business Performance

Regulatory compliance is an opportunity to build credibility and trust with your customers by reinforcing your commitment to data protection and privacy. ActionIQ is here to help guide you through the changing regulatory landscape and thrive in today's customer-centric experience economy.

The information provided in this brief is for general informational purposes only. ActionIQ does not and is not intended to provide any kind of legal advice.

More information on ActionIQ's security practices can be found in the ActionIQ Security Brief.

ActionIQ

About ActionIQ

ActionIQ is at the center of a data-driven revolution that is changing the way brands think about customer experience, digital transformation and the value of customer data as a core corporate asset. We concentrate on solving enterprise data challenges so that teams are empowered to create authentic customer experiences across all brand touchpoints. ActionIQ helps enterprise companies by connecting their first-party customer data, providing an easy-to-use interface for business users to access customer insights and enabling customer experience orchestration across channels. We are helping brands like The New York Times, Pandora Media, The Hartford, Shopify, American Eagle Outfitters and others grow customer satisfaction and revenue.

AMERICAN EAGLE OUTFITTERS AUTODESK Albertsons CONDÉ NAST e.l.f. GoPro

M&T Bank pandora shopify THE HARTFORD The New York Times