CCPA COMPLIANCE

Accurate, continuous defensibility to meet California Consumer Privacy Act compliance requirements

1525 4th Avenue, 5th floor Seattle, WA 98101-1607 - USA

+1 (206) 539-2145 sales@integris.io @integrisio

integris.io

CCPA COMPLIANCE

Accurate, continuous defensibility to meet California Consumer Privacy Act compliance requirements

- Maintain control over the use and transfer of customer data
- Protect your customers' privacy and your company's reputation

CCPA goes beyond GDPR in its definition of personal information

Requirements for the California Consumer Privacy Act (CCPA) go into effect on January 1, 2020.

Like GDPR, the CCPA is broad in its definition of "personal information."

It defines it as personal information that "could reasonably be linked, directly or indirectly, with a particular consumer or household."

You won't find the word "household" in GDPR.

It implies that personal information doesn't have to be tied to a specific name or individual (think home address, home devices, geolocation data, home network IP addresses, and the like).

GDPR lesson learned? Don't do the same work twice.

Many companies started preparing for GDPR by hiring lawyers and consultants to do impact assessments, map out workflows, conduct surveys, and introduce internal guidelines. This documentation is certainly important.

But operationalizing GDPR and CCPA requires applying this knowledge to a diverse set of data repositories—in addition to leveraging existing IT security tools, and other IT systems (e.g., SIEM, ticketing, data governance).

In today's world of data-intensive business operations and big data, compliance requires real-time, automated knowledge about your data and data flows. Thus, it's critical to get your CTO, CISO, data governance team, and chief privacy officer together to do it right the first time.

Five things to do to prepare for CCPA

1. Establish a team, define responsibilities, and get your CxOs on the same page (business and technologists).
2. Know which personal data you have and where it resides. Account for all data types—both at rest, and in motion as it enters and leaves the company.
3. Understand why and how you're using your data, and be able to map it back to obligations such as CCPA and GDPR.
4. Assess existing ticketing tools and other applications to help accelerate consumer data access requests.
5. Operationalize and automate early. Use CCPA as an opportunity to apply data privacy automation to support your GDPR compliance program, third-party data sharing agreements, and internal data use policies—on both personal information and intellectual property.

   Once you have an accurate inventory of your data, you can reallocate scarce resources to better protect your most sensitive assets.

Integris Software delivers accurate, continuous defensibility to meet CCPA

Using Integris Software, you can identify and tag personal data across any system, apply regulatory rules and contractual obligations, assess risk, and take action.

Map

Connect to any structured or unstructured data source, at rest or in motion, in the cloud or on-premises, and use machine learning and natural language processing to create a live map of your data.

Monitor

Continuously monitor your compliance efforts against CCPA, GDPR, consumer data access requests, data sharing agreements, contractual obligations, internal data management policies, and more.

Control

Kick off workflows with your existing ticketing system to remediate issues on the fly. Ensure that data governance and data management systems are accurate and current.

1525 4th Avenue, 5th floor Seattle, WA 98101-1607 - USA

+1 (206) 539-2145 sales@integris.io @integrisio

integris.io

Highlights of CCPA requirements, challenges, and how Integris responds

Section	Summary Description of Requirements	Data Privacy Management Challenges	Integris Responds
1798.100 1798.175	**The Right to Access, and Applicability** Consumers have the right to request that a business that collects their personal information disclose the categories and specific pieces of personal information it has collected. Personal information isn't limited to what's collected electronically or over the internet; it also applies to the collection and sale of all personal information collected by a business about a consumer or household. Personal information can also include inferred data used to create a consumer profile.	Not all personal data has an obvious tie back to a user ID (e.g., household data, GPS locations, voice to text, or follower lists on Instagram). Personal data has an evolving nature. What's considered a sensitive category or piece of data today may not be considered sensitive tomorrow, and vice versa. Understanding inferred personal information is important, yet challenging. For example, food choices on an RSVP card can infer religion. The number of sensitive data categories a business needs to track varies widely depending on its industry and specific business type. Categories will often fall into different classifications and schemas (depending on the organization) and have different handling and access restrictions. Companies may need to limit the sale or transfer of personal information based on its classification level.	Integris will never ask you to send us large customer data sets, because we assume all data is identifiable—even if it's not directly tied to user IDs. By using a combination of contextual awareness, natural language processing, and machine learning, we map all sensitive data elements for complete and accurate results. Using machine learning, our deeper inspection identifies data down to the data element level so as to assess privacy, integrity, and handling violations. Your data privacy landscape includes a detailed understanding of personal data categories, classifications, and individual data elements—including derivative personal data. You can even create your own definitions of sensitive data or let our machine learning make suggestions for you. Integris' ability to handle data in motion is key to helping you understand which data is entering or leaving your organization via data sharing agreements, and the streams and feeds your data scientists rely on for continuous innovation.
1798.110 1798.135	**Right to Request Disclosure of Information Collected, and Compliance Obligations** A consumer shall have the right to request that a business that collects personal information disclose to the consumer the categories of third parties with which it shares personal information, and the specific pieces of personal information it has collected. For consumers who exercise their right to opt out of the sale of their personal information, businesses must refrain from selling it.	There's often a disconnect between what has been agreed to on paper by lawyers and what's happening with the actual data. Often times, the people who negotiate the contract differ from those shipping the data, causing public embarrassment and loss of consumer trust. Also, the way contracts are written is not necessarily the way data is represented. The word "location" might appear in a contract, but the data set contains latitude and longitude values.	Integris continuously monitors your personal data against data sharing agreements and ties relevant information back to contractual obligations. We help you identify data and assign it to categories, giving it classifications such that you have granular control over the use and transfer of customer data. Enterprise multi-tenancy allows you to handle different views of the data. This lets subsidiaries manage their data separately, but still roll up under a master view.

Highlights of CCPA requirements, challenges, and how Integris responds

Section	Summary Description of Requirements	Data Privacy Management Challenges	Integris Responds
1798.105 1798.120 1798.130	**Right to Deletion, Right to Opt Out, and Disclosure Obligations** Consumers have the right to request that a business delete personal information it has collected about them. Consumers can, at any time, direct a business that sells personal information to third parties to not sell their personal information. This is referred to as the right to opt out. Businesses need to be able to associate information, provided by a consumer in a verifiable request, to any personal information previously collected by the business about that consumer.	Not all personal data is tied to a user ID. Even without an ID the individual can still be identified in a data set. By simply mapping IDs to pre-existing metadata, businesses run the risk of creating a false sense of security about the data they have, which security parameters are being applied, and whether they're in compliance with any regulatory mandate.	Integris operates at the data element level to inform you exactly what personal information is in your data set, not just what the metadata implies. The result? We're able to support your consumer data access request efforts and map personal data back to a specific consumer for complete and accurate results. In addition, we can flag issues relating to data residency and retention, misclassification and mislabeling, and security issues, such as lack of encryption for highly sensitive data. Integris makes it easy to respond to customer data access requests. Customer service reps can input data, find requested information, and share it back out with customers. They can preview customer data access request reports, add private notes, and send them to the next step in your workflow. Integris integrates with your existing ticketing system, and provides detailed logs for internal audits and compliance needs.

Get started with Integris Software's CCPA Preparedness QuickStart Program

Integris Software is the global leader in data privacy automation. By working securely, at scale, and no matter where your data resides, we provide an accurate and continuous picture of your organization's data privacy landscape.

Call +1 (206) 539-2145 or email sales@integris.io today to learn more about our CCPA Preparedness QuickStart Program.