TrustArc

SOLUTIONS BRIEF

# Managing Privacy Compliance in the Cloud

The complexity and number of regulations addressing data privacy continue to increase significantly. Companies offering cloud-based services must comply with these regulations or risk losing business due to customer trust issues and potential fines or other legal action. Compliance with regulations like the GDPR, CCPA, and CPRA requires companies to address a wide range of items, including privacy assessments, cookie consent, and data subject access requests.

*Managing Privacy Compliance in the Cloud* provides a high-level overview of privacy requirements facing many cloud companies, as well as solutions to help manage compliance.

**This document is intended as a general overview of the subject and cannot be regarded as legal advice. The information was based on the state of the market on the date the document was published.**

## Privacy Compliance is Getting More Complex

The digitization of data has inevitably led to a myriad of data privacy laws that span the globe. These regulations must be considered when doing business in the respective countries and regions to which the rules apply. **Below is just a sampling of data privacy regulations that have been introduced in recent years:**

- The General Data Protection Regulation (GDPR), which took effect in 2018 across the European Economic Area (EEA)
- All 50 U.S. states now have data breach notification laws
- The California Consumer Privacy Act (CCPA) went into effect January 1, 2020, and has been amended through the California Privacy Rights Act (CPRA), effective January 01, 2023.
- In total, 5 omnibus U.S. State privacy laws are coming in 2023: California, Colorado, Virginia, Utah, and Connecticut.
- The Brazil General Data Protection Law (LGPD)
- Canadian data breach notification, risk assessment, and reporting requirements updates
- The Turkey Data Protection Law

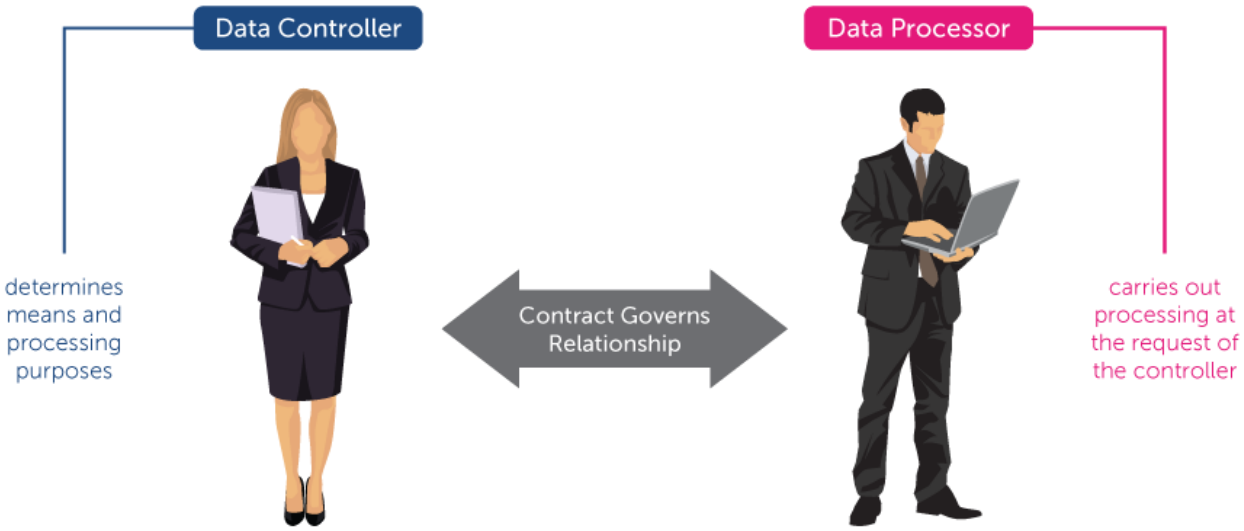
Cloud-based services are in a unique position in that they may play a dual role when it comes to data privacy management. These services may determine how personal data is processed, and they also may perform the actual processing of that data.
Cloud-based services may be both:

- **Data Controllers** - Determining the purposes and means of processing personal data and
- **Data Processors** - Processing personal data on behalf of a data controller.

## Examples of Cloud-Based Service Categories:

CRM - Customer Relationship Management
ERP - Enterprise Resource Management
HCM - Human Capital Management
PLM - Product Lifecycle Management
SCM - Supply Chain Management
SFA - Sales Force Automation

This potential dual responsibility requires providers of cloud-based solutions to pay special attention to data privacy - both in terms of establishing trust among themselves, their customers and end users - as well as regulatory compliance with current and future data privacy laws.




### Key Accountabilities

- Implement appropriate and effective measures for compliance
- Demonstrate compliance
- Provide notice to data subjects about processing: who, where, why
- Communicate with regulators about a data breach
- Vet processors
- Approve sub-processors
- Pay fines (if necessary}

### Key Accountabilities

- Implement appropriate and effective measures for compliance
- Demonstrate compliance
- Conducts processing on documented instructions
- Person(s) processing committed to confidentiality
- Support controller with breach notification
- Returns or deletes data at request of controller
- Vet sub-processors
- Pay fines (if necessary)

# Establishing and Maintaining Trust as a Cloud-Based Service

Aside from financial penalties and other compliance-related considerations, many businesses will require their vendors to be fully compliant with applicable data privacy regulations as a pre-condition to doing business. These requirements will typically be part of the RFP/vendor selection process and through privacy and security audits. Non-compliance could lead to a significant loss of business to competitors who can demonstrate their compliance.

While regulatory compliance can be considered a "price of doing business" by some, adherence to regulations can produce an environment that delivers a level of trust that will attract and retain customers.

Regarding cloud-based services, trust is the linchpin among the cloud company, customer, and end user.

- **As a Cloud-based company**, your customers are contracting for permissions to access your software as a service instead of controlling everything via an on-premise solution.
- **As a business using cloud-based services**, you entrust a third-party provider with your confidential client and company data.
- A**s an end user/end customer**, you trust that the business using cloud-based services protects your sensitive information.

By following regulations, such as the CCPA and the GDPR, you can have more confidence that you're not only going to be in compliance but also delivering the needed level of trust to everyone involved.

## Financial Implications of Non-Compliance

Under the CCPA and CPRA, in-scope businesses are subject to civil action by the California Privacy Protection Agency (CPPA). In addition to a possible injunction, infringing businesses can face penalties of up to $7,500 per intentional violation or up to $2,500 per unintentional violation.

The CCPA also provides a private right of action to California residents when non-encrypted or non-redacted personal information is subject to unauthorized access and exfiltration, theft, or disclosure due to the business's violation of security obligations. Residents may bring a private action where businesses would face paying between $100 to $750 per resident or incident, regardless of whether actual damages are shown.

The GDPR also has significant penalties for non-compliance, including fines of up to 20,000,000 euros or 4% of the total worldwide annual company revenue of the preceding year (whichever is higher).

These penalties do not include any loss of business, brand trust, or goodwill that may accompany non-compliance violations or internal/external legal fees associated with responding to an inquiry.

# Privacy Compliance Requirements for Cloud Companies

Below are some key aspects of recent data privacy regulations to consider when creating a privacy compliance program for your organization. The focus of this brief is on the GDPR and the CCPA | CPRA, as they are currently the top compliance priorities for most companies. Still, similar elements also apply to other privacy regulations.

## Expanded Territorial Scope

Recent privacy regulations have taken an expansive view of where their provisions apply by covering not only the locality where they originate but also potentially any company or organization conducting business with its residents--regardless of where that entity is based or operates.

### CCPA and CPRA

Beginning on January 01, 2023, the CCPA and CPRA apply to all companies--whether based in California or not--that have:

1) at least $25 million in annual gross global revenue during the prior year;

2) buys, sells, receives, or shares for commercial purposes the personal information of 50,000 or more consumers, households or devices; or

3) derives 50% or more of its annual revenues from selling or sharing California consumers' personal information.

### GDPR

The GDPR, which went into effect on May 25, 2018, goes beyond other earlier regulations in that processing of personal data does not necessarily have to be conducted within the European Union's borders to fall under the purview of the law. The GDPR, unlike its predecessor, the Data Protection Directive, directly applies to data processors--as many cloud-based vendors operate as--and has an extraterritorial reach provided certain conditions are met (such as offering goods and services to EU data subjects or monitoring their online behavior while in the EU).

## Privacy Program Assessments

No matter a company's industry, organizational size, or the maturity of its privacy program, conducting regular privacy assessments is important to understanding and facilitating compliance. These assessments need to address a wide range of legal requirements and best practices and will help build an action plan to identify gaps and define and manage remediation activities.

## Consent

Under the GDPR, data subject consent is a lawful basis of processing that many companies rely on before any collection or processing of data occurs. Organizations are required to state their request for consent in clear, concise terms that can be understood by anyone visiting their site or using their services. If relied on, consent must be a freely given, specific, informed, and unambiguous indication of a data subject's agreement to the processing of personal data relating to him or her, and consent must be as easy to withdraw as it was to obtain.

Similar to the GDPR, under the CCPA, businesses are allowed to sell minors' data based on opt-in consent. Businesses may enter a consumer into a financial incentive program only if the consumer provides the business revocable, prior opt-in consent.

## Individual Rights

Privacy laws such as the GDPR and the CCPA seek to protect the personal data and privacy of individuals (also known as "data subjects" or "consumers," respectively). CCPA provides for the following data privacy individual rights:

- **Access:** Individuals may request disclosure of the specific data elements of personal information collected about them, categories of personal information collected, categories of sources, purposes for collecting or selling, and categories of recipients with whom the personal information has been shared
- **Data Portability:** If the specific data elements of personal information are provided to the requestor electronically, to the extent technically feasible, they must be provided in a readily transferable electronic format
- **Deletion:** Individuals may request to have their personal information deleted
- **Disclosures about Sharing/Sale:** Individuals may request an accounting of the disclosures, including the sale, of personal information made to third parties; this significantly expands upon existing California "Shine the Light" law

- **Opt-Out:** Individuals may object to the sale of personal information about them. The CPRA updated CCPA to include a new category of personal information: **Sensitive Personal Information**, and the right to limit and opt out of its use.
- **Opt In:** Minors, or their guardian, must affirmatively authorize the sale of the minor's personal information
- **Correction:** Consumers may request that inaccurate personal information be updated.

The GDPR has also **given consumers the right to access the data collected from them** by data controllers.

The GDPR states that access requests should generally be granted, without a fee, in an electronic format, and within a month of the request. For example, the "right to erasure" (also referred to as the "right to be forgotten") allows a customer to request that a data controller holding personal data about the customer erase it without undue delay if certain GDPR Article 17 conditions are met. If this request is sent, any third-party services need to stop processing that customer's personal data as well.

## Breach Notification

Per the GDPR, if any personal data breach occurs that may result in a risk to the rights and freedoms of individuals, it needs to be brought to the attention of the proper supervisory authority without undue delay and within 72 hours of the company becoming aware of the breach. Likewise, data processors must notify data controllers without undue delay after becoming aware of the breach. All breach activity and responses need to be captured in audit logs for tracking and archiving purposes.

## Data Inventories, Records of Processing Activities, and Data Flow Mapping

One of the most important steps in designing and building a data governance or privacy program is to create an inventory of all of the business processes within a company. If a company does not know the type of data it collects, buys, or imports or how it's processed, shared, sold, or stored, it is difficult to know whether that company is meeting the requirements of the privacy frameworks applicable to its business. It is also difficult to know where data resides to be able to respond to data subject access requests efficiently.

# TrustArc Can Help You Achieve Compliance and Establish Trust

TrustArc offers a broad range of solutions to help companies build and manage a privacy program, including the TrustArc platform, consulting services, and certification/validation programs that can be tailored to meet your business needs.

## Privacy Readiness Assessments

For many companies, the best place to start is by conducting a readiness assessment. TrustArc offers multiple readiness assessment options designed to help companies determine what regulations apply to their business and help them determine the next steps on the path to compliance. Assessments are powered by TrustArc Assessment Manager and can be led by an expert TrustArc consultant.

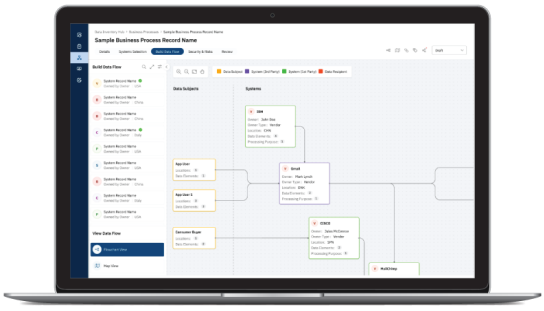
The assessments include a detailed review against regulatory requirements and deliver a comprehensive summary of gaps, remediation recommendations, and a prioritized step-by-step implementation plan to achieve and maintain compliance. After assessing compliance risks, TrustArc can help build processes and implement tools to manage privacy requirements. The TrustArc platform addresses a wide range of privacy compliance requirements.

## TrustArc Platform

The TrustArc Platform is comprised of the following modules:

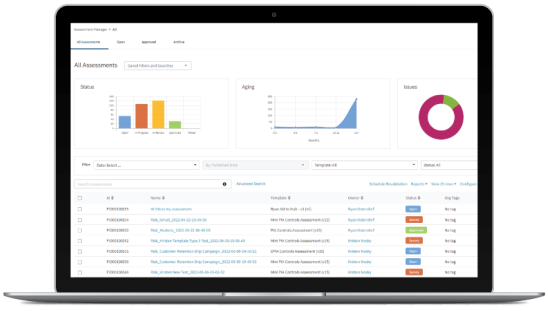
### Data Inventory Hub

Create and manage a data inventory, which is essential to understanding data flows, assessing risk, and managing individual rights



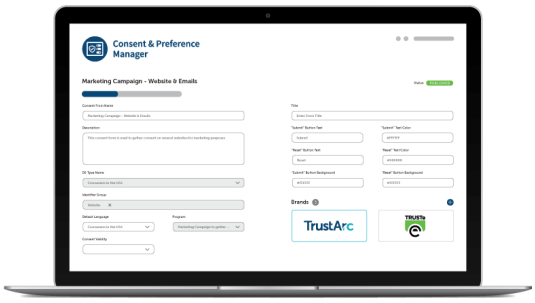
### Assessment Manager

Conduct ongoing privacy risk assessments, including PIAs and DPIAs



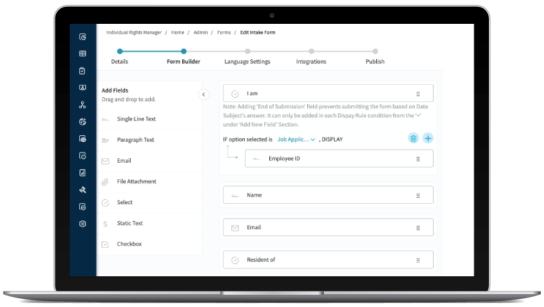
## Cookie Consent Manager

Manage cookie consent obligations




## Individual Rights Manager

Manage data subject access requests (DSAR)




## Website Monitoring Manager

Identify and manage first- and third-party tracking technologies across all websites


## TrustArc Cloud Industry Experience

TrustArc has worked with hundreds of cloud-based service providers across all industries. We bring extensive industry expertise and are uniquely positioned to help you build and manage a compliant privacy program.


## Manage Privacy Compliance in the Cloud with the TrustArc Platform

**Schedule a Tailored Consultation**

## About TrustArc

As the leader in data privacy, TrustArc automates and simplifies the creation of end-to-end privacy management programs for global organizations. TrustArc is the only company to deliver the depth of privacy intelligence, coupled with the complete platform automation, that is essential for the growing number of privacy regulations in an ever-changing digital world. Headquartered in San Francisco and backed by a global team across the Americas, Europe, and Asia, TrustArc helps customers worldwide demonstrate compliance, minimize risk, and build trust. For additional information, visit www.trustarc.com.