TrustArc
Privacy Compliance

Essential Guide to the CCPA

How to Build, Implement, and Demonstrate CCPA Compliance

TrustArc Simplifies Privacy Compliance and Risk Management

Extensive Use Cases

GDPR
CCPA
HIPAA

All Maturity Phases

Build
Implement
Demonstrate

Comprehensive Solutions

Platform
Consulting
Certification

Flexible Delivery Options

Self Service
Managed Service
Hybrid

This guide distills the California Consumer Privacy Act (CCPA) into discrete phases to help a business achieve and then maintain compliance. The guide is designed for professionals across a wide range of functions who will be impacted by the CCPA. As with all regulatory matters, please consult with your legal team to ensure your plans are consistent with internal guidelines and requirements. If you have questions on any information in this guide, or want to get an update on emerging CCPA news, please contact a TrustArc representative.

Whatever your team decides, your CCPA plan also needs to account for the unexpected. Invest time upfront to perform the proper analysis and planning, so that you can be confident your company's CCPA compliance program will efficiently and effectively mitigate risk while meeting business objectives.

GDPR Compliance Roadmap - 5 Phases

Build Program and Team	Assess Risks and Create Awareness	Design and Implement Operational Controls	Manage and Enhance Controls	Demonstrate Ongoing Compliance
Identify Stakeholders	Conduct Data Inventory & Data Flow Analysis	Obtain & Manage Consent	Conduct PIAs (DPIAs)	Evaluate & Audit Control Effectiveness
Allocate Resources & Budget	Conduct Risk Assessment & Identify Gaps	Data Transfers & 3rd Party Management	Data Necessity, Retention & Disposal	Internal & External Reporting
Appoint DPO	Develop Policies, Procedures & Processes	Individual Data Protection Rights	Data Integrity & Quality	Privacy Notice & Dispute Resolution Mechanism
Define Program Mission & Goals	Communicate Expectations & Conduct Training	Physical, Technical & Administrative Safeguards	Data Breach Incident Response Plan	Certification

Sample Timeline

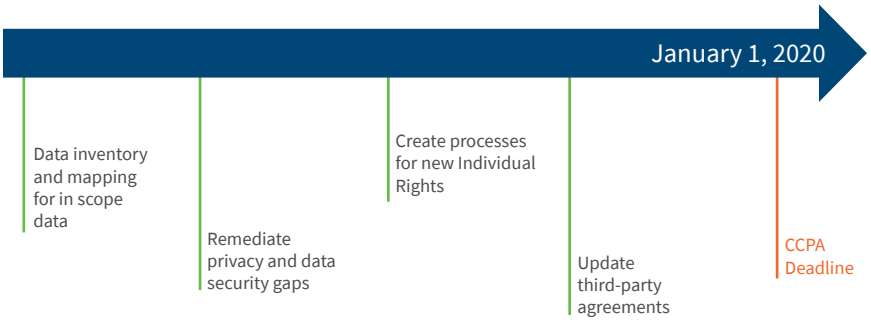


Table of Contents

Chapter I: Introduction to the California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) is a bill passed by the California State Legislature on June 28, 2018, which was amended and signed into law on September 23, 2018. The CCPA is set to be the toughest privacy law in the United States. It broadly expands the rights of consumers and requires companies within scope to be significantly more transparent about how they collect, use, and disclose personal information. The CCPA is effective January 1, 2020, and enforcement is slated to begin no later than July 1, 2020.

The CCPA is one of the first laws to show that, as many jurisdictions have and are continuing to do, the U.S. may be trending toward more rigorous global privacy regulations. The CCPA has many similarities to the European Union's General Data Protection Regulation (GDPR), from its extraterritorial reach to its expansive rights for individuals, and will likely impact tens of thousands of businesses worldwide that collect California consumers' personal information.

Businesses that have prepared to comply with GDPR by creating comprehensive data governance practices, records of processing, and individual rights procedures will have a head start. But, under the CCPA, all companies in scope will need to enhance their data management practices, expand their individual rights processes, and update their privacy policies by the January 1, 2020 effective date.

The deadline for compliance is January 1, 2020

Who does it apply to?

The CCPA will apply to a business if it, or an entity it controls or that controls it, collects or receives personal information from California residents, either directly or indirectly, and meets one or more of the following criteria:

- Has annual gross revenue that exceeds US $25 Million;
- The entity annually receives, buys, sells or shares, directly or indirectly, the personal information of 50,000 or more California residents, devices, or households;
- 50% or more of its annual revenue is derived from the sale of personal information about California consumers.

Non-Compliance Implications

Fines for non-compliance can add up quickly; these fines are in addition to any loss of goodwill or consumer trust - or expenses associated with responding to any compliance investigations.

Both the GDPR and CCPA require companies to think differently about their customers and how personal data is used. Transparency and communication about where a customer's data goes or what it's used for is necessary to doing business in the digital age. The new regulations signal a shift in expectations between customers and companies, and so companies will have to work harder to gain and retain customer trust. Companies who provide customers more control and choice over their data can build customer relationships by using that as a competitive edge.

Civil penalties under the CCPA:

California's attorney general is empowered **in Section 1798.155(a) of Title 1.81.5 of the CCPA** to bring an action against any company or individual person violating the Act. The CCPA allows for fines of up to $2,500 per violation or $7,500 per intentional violation, but does not place a cap on the total amount of fines. The CCPA provides businesses with a period of 30 days to remedy alleged violations of the law before a fine can actually be assessed.

For example, under the CCPA, a violation impacting 10,000 California consumers could carry a penalty of $25 million for an unintentional violation and as much as $75 million for an intentional one.

Private right of action:

The CCPA also offers a private right of action that allows consumers to seek statutory or actual damages if their sensitive personal information is subject to unauthorized access, theft or disclosure as a result of a business's failure to implement and maintain required reasonable security measures. It does not apply if the personal information is redacted or encrypted. Statutory damages can be between $100 and $750 per California resident "per incident," or actual damages, whichever is greater.

Chapter II: How to Comply

The CCPA and California A.B. 1906 (Security, Privacy of IoT Devices) were both passed soon after the EU General Data Protection Regulation, and continue the trend of California leading the U.S. in legislating compliance standards. The GDPR set the stage for more choice, more transparency, and more mature privacy programs to protect personal information. Enhanced individual rights (such as access and deletion), additional transparency requirements, and required security measures are all causing companies to re-evaluate their security and data management programs from the bottom up.

Companies that have gone through a large compliance effort in the past (e.g., GDPR or ISO Certification) likely will have fewer gaps to resolve to prepare for the CCPA, but all companies in scope will have some work to do.

Before building a program, TrustArc suggests that companies review with legal counsel all applicable privacy compliance regulations or frameworks with which your company will have to comply. Finding commonalities between the requirements and controls will allow a company to find overlap between the obligations, and then adjust for any differences, rather than having completely separate programs.

The following chart highlights a subset of requirements that are similar for both the CCPA and GDPR. The first column provides the general area where each law has requirements that pertain to a particular subject area, for example, data subject rights. The second column summarizes the applicable CCPA requirements, and the third column summarizes the GDPR requirements. The last column provides a sample best practice to follow.

Privacy Requirement	CCPA Requirements	GDPR Requirements	Best Practice
Transparency	A business (controller) is under an obligation to provide consumers information such as the categories of personal information to be collected; the purposes for which the personal information will be used; and the categories of third parties with whom the business shares personal information. Include this information in the businesses privacy policy and update the policy at least once every 12 months.	A controller is under an obligation to provide details such as its identity and contact details; any recipients of the personal data; and the intended purposes of processing the personal Information. Include this in a policy or notice such as a privacy notice or a GDPR-specific policy.	The compliance standard for transparency obligations is more rigorous for the GDPR, but both GDPR and CCPA require updates to your business's privacy notices/ policies. Ensure your notices are updated at least annually, meet the transparency requirements of any applicable laws, and formally document that process.
Processor Obligations	Businesses (controllers) are required to convey deletion requests to their service providers. Service providers are liable for civil penalties under the CCPA. Otherwise, obligations for "processors" are much more rigorous in the GDPR.	There are detailed requirements for controllers on how to evaluate, engage, and manage processors. Processors also have obligations, and are liable for civil penalties for failure to comply	Controllers and their processors have obligations under both the GDPR and CCPA. If your organization is a controller, ensure that you have evaluated the processors you engage and that contracts are in place with the processors. If your organization is a processor, ensure you have the requisite processes and mechanisms in place to support controllers in meeting their obligations to individuals.

Privacy Requirement	CCPA Requirements	GDPR Requirements	Best Practice
Individual Rights: Data Portability and Data Access	The CCPA provides consumers the rights of access and data portability. Consumers have the right to obtain from a business their personal information, including the categories and specific pieces of information collected; the categories of third parties with whom information is shared; and the categories of sources from which the information was obtained. Consumers also have the right to obtain their personal information in a format that allows the consumer to transmit it to another organization. Businesses need to respond within 45 days.	The GDPR provides individuals the rights of access and data portability. Individuals have the right to receive confirmation from a controller about whether personal data about them is being processed; and, if so, additional information, including the categories of personal information concerned; the recipients or categories of recipients with whom the information has or will be shared; and the purposes of processing. Organizations need to respond within one month of receipt of the request.	The GDPR and CCPA both have the individual rights of access and data portability. Ensure that these types of requests are managed and your processes documented. Review your current process and mechanisms that are in place to respond to access requests. Assess their efficacy. Address compliance gaps and use technology tools to automate manual processes to scale and simplify.
Individual Rights: Deletion	The CCPA provides consumers the right of deletion. Consumers may request that businesses delete their personal information.	The GDPR provides individuals the right of deletion, or “the right to erasure.” Organizations need to process deletion requests within one month of receipt of the request.	The GDPR and the CCPA both have deletion obligations. Review the types of data your company retains, and the legal basis for processing it. Ensure effective processes and mechanisms are in place to respond to deletion requests. Address compliance gaps and use technology tools to automate manual processes to scale and simplify.

Overview – People, Process, & Technology

For all phases, use a combination of your team, a defined process, and technology tools.

People - Identify the team members who will be responsible for conducting the tasks and whose informational inputs are necessary for a comprehensive assessment. Ensure that everyone involved is trained on the process and technology. Ideally team members will be well versed in data privacy management requirements and best practices.

Process - Design the workflow of information gathering and identify gaps against the requirements. Leveraging best practices and templates in questionnaire form instead of manual checklists will build efficiency. A business will likely need multiple templates to address different types of risk; however, a single template may be effectively used to address a set of processing operations that present similar high risks.

Technology - Privacy technology platforms with built-in digital data discovery, data inventory, DPIA / PIA and assessment templates, cookie consent, workflows, and reporting will enable a team to collaborate, guide the workflow process, serve as the central repository of compliance evidence, and facilitate ongoing periodic audits that reflect business changes.

Phase 1 – Build Consensus and a Team

Begin by going back to the stakeholders you first spoke to when determining whether the CCPA applies to your company. Key stakeholders may reside in these departments:

- Engineering
- Human resources
- Information security
- Legal
- Marketing
- Procurement
- Product management
- Website development

With help from these stakeholders, you can gain a high level understanding of your current compliance posture. You need to compare your current practices against a comprehensive list of the requirements, including the following areas.

GDPR Overlap

Similar to the GDPR, the CCPA will require organizations to focus on personal information and provide transparency in their practices around that data. Certain CCPA requirements overlap with the existing GDPR individual rights requirements, which may be useful for GDPR-ready organizations. However, existing privacy notices, even those updated for the GDPR, will not automatically be CCPA "ready" and will need to be reviewed and updated.

Vendor Management

Contracts with third parties with whom personal information about California residents is shared will need to be updated to comply with CCPA requirements. Third-party data processors whom companies rely upon will need to ensure they are meeting CCPA compliance. Take steps to require documentation of processing activities and security standards / 3policies and also ensure there is a distinction between the transfer of data for processing purposes and the transfer of data for a sale.

Look Back Period

The budget should take into account supplying your team with the resources necessary to address the requirements around access, accounting of disclosures, and transparency requirements. For example, companies will have to identify any personal information previously collected by the business about the consumer for the past 12 months, so the process should ensure that business processes that collect personal information are recorded in a data inventory. A company will need to be able to identify the type of personal information being collected; there are 11 categories enumerated in the CCPA and the company would have to choose the one that most closely describes the personal information. The company will also need to know why it collected the personal information (the purpose); which categories of personal information were sold; and which categories were disclosed for a business purpose. Keeping up-to-date and detailed records will be key.

Individual Rights / Consumer Rights

With regard to the CCPA, enhanced individual rights (such as access and deletion), additional transparency requirements, and required security measures are all causing companies to re-evaluate their security and data management programs from the bottom up. These rights may require companies to develop new processes and implement technology - based solutions to receive, escalate, and accommodate requests.

Phase 2 - Assess Risks and Create Awareness

Conduct a Comprehensive Data Mapping Analysis

To help ensure you have uncovered all of the risks and appropriately prioritize your plan, you must have a solid understanding of your organization's complete data lifecycle. The process to document this lifecycle is referred to as a data inventory analysis or data flow mapping. This process generally involves:

- Gathering information from key contacts across the company about what information they collect and use, how it is used, where it is stored, how it flows through and out of the company, who has access to it, and what protections are in place at each point; in other words, gather details about data collection, storage, usage, transfer, processing, and disposal.
- Documenting this information in the form of inventories of data and visual "maps" of the data movement.
- Analyzing risk points and triggers for various CCPA or other requirements.

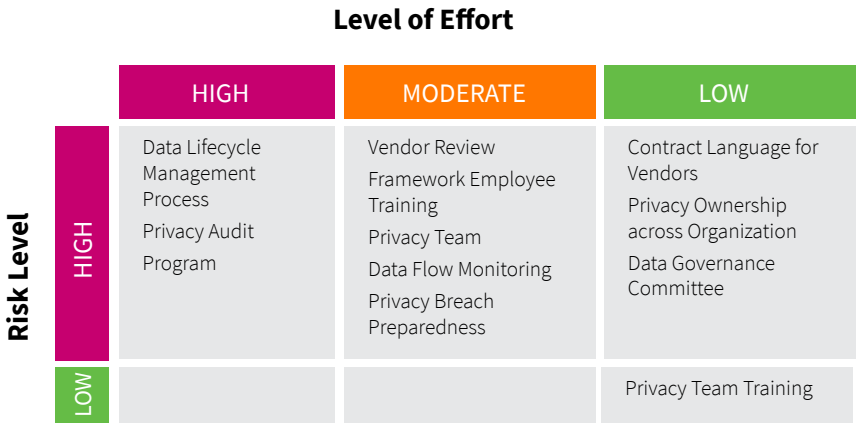
Getting Buy-In

Getting buy-in requires you to speak the language of the department you are trying to engage. Here are some examples:

- Information Technology: identifying storage redundancies can reduce IT complexity and save IT dollars.
- Information Security: understanding what data resides in which systems can help InfoSec prioritize their protection efforts and establish appropriate access controls.
- Operations: visualizing flows and uses of data throughout the company can help Operations identify redundancies and improve efficiencies.
- Procurement: identifying points at which the company shares information with third party vendors and understanding the sensitivity of the data being shared can help Procurement approach third party management and contracts in a risk-based, efficient approach.

Conduct Gap Assessment and Assign a Level of Effort

With the results from your Data Inventory you can now conduct a Gap Assessment and develop a Level of Effort (LOE) Matrix to help prioritize what needs to get done first. The table below illustrates sample Level of Effort (LOE) estimates – Low, Medium, and High, which will help visualize your plan's priorities.



Risk Level vs. Level of Effort

Develop Policies, Procedures, & Processes

Armed with the results of the Gap Assessment and understanding of the Level of Effort required to address these gaps, assign tasks to each functional area within the business with a timeline for completion. The risk and Level of Effort associated with each gap can inform task scheduling, with high risk items prioritized first and tasks requiring significant levels of effort begun in advance of easier ones.

Most companies will find that policies, procedures, and training are critical components of filling in CCPA compliance gaps. Documenting expectations for employees and vendors, carefully describing how individuals should apply those expectations in their daily work lives, and training individuals so that they have the ability to apply those expectations are essential to compliance with the CCPA. Remember also that it is not enough to conform to data handling requirements under the CCPA – your company also must be able to demonstrate that it conforms.

Communicate Expectations

Building consensus up-front is critical to the success of any privacy program within an organization, especially a program addressing the complexity of the CCPA. Fundamental leadership principles and organizational decision-making must come into play. Given the expanded scope of the CCPA and likely higher investments required to comply, building consensus will be critical to secure funding.

Make the Case

Approach this process like building any business requirements case by developing a narrative that shows the pros and cons of making the investment. You should use these key communication strategies to establish a compelling story for your CCPA compliance efforts:

Develop the Pitch

"The CCPA Impacts our Company…Posing Threats and Opportunities"

- Fines and / or expenses responding to regulatory inquiries
- Lost business due to inability to meet customer and partner privacy / security standards
- Loss of goodwill and damage to brand
- Lost business versus companies using strong privacy posture as a competitive advantage

"Our Company Has Compliance Gaps That Require Remediation"

- Initial CCPA Readiness Assessment results identified multiple gaps and risks
- Cite any internal history of privacy breaches, regulatory inquiries, or enforcement actions

"Our CCPA Compliance Program Will Require New Investments"

- Proposed project overview with timeline, methodology, and metrics
- Outline the personnel, tools, training, and new processes required
- Benchmark reports depicting CCPA actions by competitors

Share the Pitch with Key Stakeholders

Facilitate an internal kickoff and ongoing planning sessions with relevant stakeholders across the organization. Include representatives throughout the company including colleagues at executive and board levels. Build and deliver an engaging presentation leveraging all of the evidence you gathered to tell the story. Involve any department that touches customer or employee data, whether they are on the collection end or simply have access to the data.

At the outset, it will be important to clearly state the following goals of the kick-off session:

- Formalize CCPA program team structure / roles / responsibilities
- Establish the CCPA program as a priority initiative
- Agree on short, medium, and long-term goals of the CCPA program
- Set measurable objectives with success criteria and key milestones
- Secure budget and resources based on Level of Effort estimates

If your company already has a Privacy Working Group, this campaign would be an add-on to that existing process. If your company does not have a working group, building one will provide ongoing value for years to come. Schedule ongoing planning meetings with a regular cadence to develop the full plan, implement all required operational changes, and provide a dashboard report on the CCPA program's progress.

Once everyone understands the urgency, conduct training to help stakeholders understand what is required and the types of changes your company will be making.

After you have completed your plan and achieved organizational support, you can begin to implement the various components required to operationalize your compliance. These will include a range of initiatives, from hiring new personnel, training existing personnel, establishing new processes, and implementing new technology.

Many of these items can be completed in parallel, depending on your organization's resources and risk status as outlined in the planning cycle. The time to complete this phase will vary greatly by company size, budget, and compliance gaps.

Phase 3 – Design and Implement Operational Controls

Consent

There are several rights related to consent that should be reviewed when designing your CCPA compliance operational controls. A consumer has the right to direct a business that sells personal information to not sell their personal information (PI). For businesses engaged in selling this type of data they will need to put in place controls to manage the opt-out request (where they must stop selling data) and also a process to capture subsequent authorization if the consumer changes their mind in the future.

In the case of children who are less than 13 years of age, businesses are also obligated to obtain opt-in consent from a child's parent or guardian before selling their PI.

Additional controls:

- A business must respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's PI again.
- An exception does exist for PI collected in connection with a consumer's exercise of an opt-out request if the PI is solely used for complying with the opt-out request.
- A business is required to create a separate "Do Not Sell My Personal Information" webpage with a clear and conspicuous link from their homepage that directs California consumers, or a person authorized by the consumer, to opt - out of the sale of the consumer's PI.
- A business must also be able to "reasonably verify" requests; for example, the CCPA provides that a request made via a consumer's password protected account with the business is considered a verifiable consumer request.
- Businesses should build controls based on what is reasonable for their environment and look for regulations to be adopted by the Attorney General.

Transparency

Consumer rights under transparency ensure that businesses must disclose what personal information they've collected and they must identify the third parties involved in both the sharing and selling of data. The following must be disclosed in online privacy notices:

- The categories of personal information that the business collected about the consumer.
- The categories of personal information that the business sold about the consumer.
- The categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold.
- The categories of personal information about the consumer that the business disclosed for a business purpose.

In addition, a business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the above. While businesses may have previously had in place some of these items, the CCPA applies these obligations to all businesses that collect personal information about California residents.

Individual Rights / Consumer Rights

Certain CCPA requirements, such as the individual rights for data deletion, data access and portability overlap with requirements previously established with the GDPR. The CCPA requires such requests be fulfilled within 45 days. Businesses also have an obligation to notify consumers of their deletion rights in a form that is "reasonably accessible" to consumers, such as within their online privacy notice.

- Right to access California personal data collected in the last 12 months
- All access requests must be exported in a "user friendly" format
- Right to opt-out of selling personal data to third parties
- Right to data deletion

Additionally, businesses must implement two (2) or more designated methods for consumers to submit requests for information including, at a minimum, a toll-free telephone number and, if the business maintains a website, a website address. Note the right to data deletion is not unlimited and the law allows for business to refuse the request for example in cases where the PI is necessary for specific reasons including to complete a contractual transaction or provide a good or service requested by the consumer.

Security and Breach Notification Obligations

The CCPA does not directly impose data security requirements, but it does establish a right of action for certain data breaches that result from violations of a business's duty to implement and maintain reasonable security practices and procedures appropriate to the risk arising from existing California law such as the California Security Breach Information Act (SB-1386).

For example, SB-1386 requires organizations that maintain personal information about individuals to inform those individuals if the security of their information is compromised. If there's a security breach of computerized consumer records containing personal data, the responsible organization must notify each individual for whom it maintained information. The statute applies regardless of whether the computerized consumer records are maintained in or outside California.

Phase 4 – Enhance Controls

Develop CCPA Program

Similar to the efforts many organizations undertook to comply with GDPR, CCPA will require companies who do business in California across technology and many other industry sectors to be accountable for their data handling practices in order to address the broad scope of individual rights similar to those under GDPR. Once the appropriate new controls have been identified (in Phase 3) and created, they then must be incorporated into ongoing compliance work so they can be routinely assessed:

- Regularly review changes to process and data flows
- Consolidate the in scope California consumer personal data as much as possible and update data inventory documentation
- Review and update data retention and deletion processes
- Develop the appropriate approvals and workflows to manage customer personal data and fulfilling individual requests
- Consider if any data security program upgrades needed to support compliance activities
- Update employee training materials to incorporate CCPA information

Best Practice Tips

TIP

- ☑ Incorporate these individual rights into your privacy program and ensure there is an established process from beginning to end.
- ☑ Take your data inventory and data processing records a step further to envision requests made for that data.
- ☑ Work with your vendors to ensure that data subject access rights can be honored on their side and get documentation to validate that ability.
- ☑ Be helpful. This is not an adversarial process. These are rights provided to individuals to protect their freedoms and right to privacy.

Phase 5 – Demonstrate Compliance

Demonstrate ongoing compliance by documenting all changes and producing compliance reports.

Summary - 10 Steps Toward CCPA Compliance

Build a Compliance Plan

1. Determine whether the CCPA applies to any part of the business, and whether the requirements related to collection, sale, or both, are applicable.
2. Conduct a gap analysis against current individual rights management policies and procedures and transparency practices.
3. Determine which business processes and activities are in scope for CCPA and which involve minors.
4. Create a data inventory of your data elements and/or update data flow maps relevant to the collection, sale, and disclosure of personal information (which are in scope).
5. Determine which CCPA individual rights apply to each business process or activity.
6. Determine whether to offer any financial incentives for the sale of personal information.

Implement the Compliance Plan

7. Develop updates to individual rights management policies and procedures.
8. Update Privacy Policies to include required disclosures under CCPA.
9. Update contracts with vendors and third parties with whom personal information is shared.
10. Implement individual rights mechanisms to effectively manage incoming requests from consumers

Chapter III: How TrustArc Can Help

TrustArc has a comprehensive set of privacy management solutions to help you manage all phases of CCPA compliance. Our solutions are powered by the TrustArc Platform along with our team of privacy experts and proven methodology.

CCPA Assessment

The first step is to assess California Consumer Privacy Act (CCPA) compliance status, identify gaps, and develop an action plan to manage ongoing compliance. TrustArc offers two assessment options:

- CCPA Privacy Assessment
- GDPR to CCPA Privacy Assessment

CCPA Privacy Program Development

After identifying risks and building a remediation plan, the next step is to design, build and implement processes and tools to address compliance requirements. TrustArc offers CCPA privacy program development services for the following areas:

- CCPA Data Inventory Program
- CCPA Risk Assessment Program
- CCPA Transparency Program
- CCPA Use, Retention and Disposal
- CCPA Third Parties and Onward Transfer
- CCPA Choice and Consent
- CCPA Children's Protection
- CCPA Access and Individual Rights
- CCPA Incident Response
- CCPA Policies and Standards

CCPA Privacy Platform

Use the TrustArc Platform to build and manage your CCPA compliance program.

CCPA Program Management Modules

Data Flow Manager

Create and manage a comprehensive data inventory and data flow maps.

Assessment Manager

Manage DPIAs / PIAs in a secure and centralized platform across your company.

Intelligence Engine

Automate, simplify, and tailor privacy program development and maturity, compliance and risk management.

CCPA Marketing Compliance Modules

Cookie Consent Manager

Manage user consent regarding the use of cookies so you can legitimately collect and store data on a user's computer.

Marketing Consent Manager

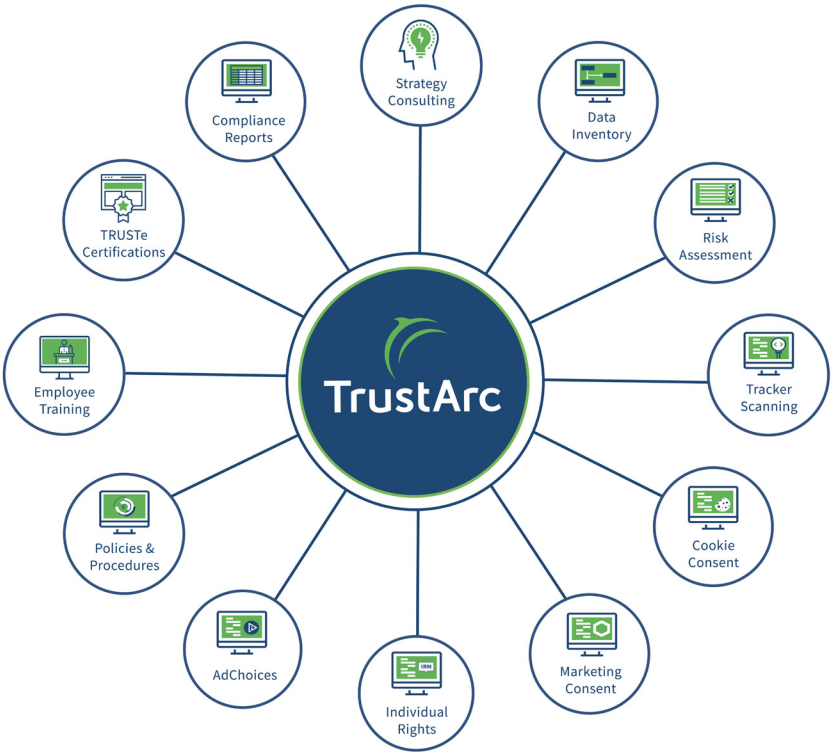
Manage consent requirements for direct marketing activities.

Individual Rights Manager

Set up the procedural and technical structures needed to address data subject rights requirements.

Why TrustArc

TrustArc provides a unique combination of deep privacy expertise, proven methodology, and powerful technology to solve complex compliance challenges like the CCPA.



Our People

The TrustArc team, located at both our headquarters in San Francisco and offices throughout the US, EU, and Asia, is dedicated to developing and delivering best in class data privacy management solutions. The TrustArc team has helped companies of all sizes across all industries develop and implement privacy programs by using its extensive privacy, legal, technology, business, and project management experience. TrustArc Privacy Consultants and Analysts are recognized data privacy leaders with significant experience using the TrustArc methodology and Data Privacy Management platform at every stage of privacy maturity.

Our Methodology

For two decades TrustArc has continuously refined its methodology to address new and existing laws, regulations, and standards. Additionally, our best practice standards are based upon helping thousands of clients at all levels of privacy maturity. Our processes are powered by our technology solutions to provide an unparalleled level of service.

Our Technology

The TrustArc Platform was purpose-built to address complex privacy compliance and risk management challenges. The award winning SaaS solution has been continuously expanded to address automated compliance reviews, cookie consent management, website tracker scanning, advertising compliance, data mapping, and much more. This proven technology solution is backed by an expert team of engineers, used by clients across all industries and available in flexible self-service and managed-service delivery options.

About TrustArc

TrustArc, the leader in privacy compliance and data protection for over two decades, offers an unmatched combination of innovative technology, expert consulting and TRUSTe certification solutions, that together address all phases of privacy program management. The TrustArc Platform, fortified over eight years of operating experience, across a wide range of industries and client use cases, along with our extensive services, leverage deep privacy expertise and proven methodologies, which have been continuously enhanced through thousands of customer engagements. 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 more information, visit www.trustarc.com.

TrustArc
Privacy Compliance

TrustArc Simplifies Privacy Compliance and Risk Management

Extensive Use Cases

GDPR
CCPA
HIPAA

All Maturity Phases

Build
Implement
Demonstrate

Comprehensive Solutions

Platform
Consulting
Certification

Flexible Delivery Options

Self Service
Managed Service
Hybrid

www.trustarc.com/CCPA

Published February 2019