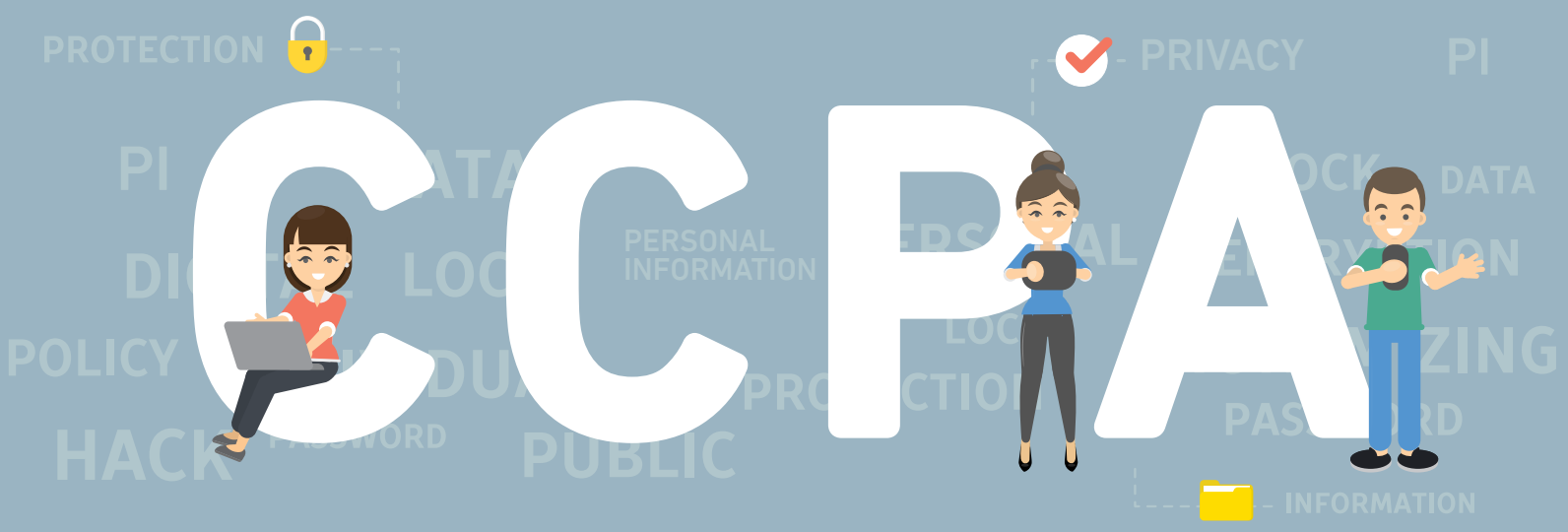
MEETING THE CCPA CHALLENGE



Now and for the Future

FIRST SAN FRANCISCO PARTNERS

Collibra

TABLE OF CONTENTS

EVOLUTION OF DATA PRIVACY AND EMERGENCE OF THE CALIFORNIA CONSUMER PRIVACY ACT

Data has become the lifeblood of our digital economy. We live in a data-never-sleeps reality where we produce 2.5 quintillion bytes of data* daily. In order to extract its full value, many organizations have embarked on a data-driven journey, not as a vague corporate sentiment but truly as a cultural shift — and anchor.

Over the last five years, the road toward data-driven business transformation has evolved to include critical navigation of a rapidly shifting data privacy landscape. In our digital world, we are creating, using and sharing data constantly — with personal information (PI) becoming a vital asset for many companies to buy, sell, disclose or trade. To regulate this economy of PI and to embrace higher standards for data protection, stringent data privacy regulations have emerged...with many more looming on the horizon.

The European Union's General Data Protection Regulation (GDPR) went into effect in May of 2018, ushering in the most important sea change in data privacy regulation in 20 years. The GDPR set new standards for consumer rights regarding their data, and brought data protection guidelines (and hefty penalties for non-compliance) to companies that collect data on citizens in the European Union.

In the wake of GDPR, the **California Consumer Privacy Act** (CCPA) was created to grant Californians similarly sweeping rights around the collection, storage, sharing and use of their personal information. The Act is effective January 1, 2020, impacting 40 million California residents and thousands of businesses that hold and/or sell personal data about them.

While the definitions, scope and requirements of the CCPA are likely to evolve, data privacy is here to stay and the impact will inevitably be broader across the U.S. as other states follow suit. The most successful organizations must not only be prepared to meet the CCPA's compliance requirements, but also quickly respond to new data privacy mandates and, most importantly, earn and maintain consumer trust in a data-driven world.

*Data Never Sleeps: Domo

UNDERSTANDING THE CCPA

Background

On June 28, 2018, Governor Jerry Brown signed the CCPA into law, protecting Californians' rights to know what data is collected by a company, how it is used, and also ensure deletion of record upon request or opt-out of data being sold.

For now, very small businesses that do not deal in PI can breathe a sigh of relief, but the universe of businesses that are covered in the scope of CCPA is still significant.

Who Must Comply

A business will need to comply with the CCPA if it is a for profit entity that...

Collects PI or Has It Collected by Others

Determines Purposes of Processing PI
(solely or jointly)

Does Business In CA
(sell goods or services to residents)

AND meets one or more of these criteria:

$25 million+
Annual gross revenue is $25 million or greater

50K or more
Works with PI for 50,000 or more consumers, households or devices

50% or more
Earns 50% or more of its annual revenue from selling PI

CCPA also applies to businesses that control or are controlled by an entity that meets the above criteria and share common branding.

Who and What is Protected

CCPA protects its state's consumers as defined here:

- "Consumer" is a natural person who is a California resident. "Natural" means an individual human being, as opposed to a legal person, which may be a private (i.e. business or non-governmental organization) or public (i.e. government) organization.
- "Resident" is defined in the tax code as being where an individual files his or her taxes. If a business cannot determine where an individual files taxes, then the business may need to assume that the individual is a California resident — effectively making the law "national."

Who and What is Protected (cont.)

CCPA protects PI meaning information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. This is a very broad definition and much more comprehensive than what is protected in the GDPR.

"Publicly available information" (i.e. lawfully made available from federal, state or local government sources) is excluded; however:

- The data sources must also be used for the purpose the data was originally maintained and shared.
- Social media and search engines are not considered to be publicly available sources.

Under CCPA, California consumers will now have certain rights related to their PI, including:

Right to Know	The Consumer has the right to ask the Business to disclose to the Consumer the Categories of PI that it has collected about them, the Categories of Sources it has collected the PI from, and the Categories of Third Parties that the Business has sold the PI to in the past 12 months.
Right to Access	The Consumer has the right to ask the Business to provide a list of the actual PI values it has collected about the Consumer in the past 12 months.
Right to Delete	The Consumer has the right to ask the Business to delete their PI.
Right to Opt Out	The Consumer has the right to ask the Business to stop selling, or disclosing for other business benefit, the Consumer's PI.
Right to Equal Service	The business cannot discriminate against the Consumer for exercising any of their rights.
Notice to Consumer	The Business must provide clear notice to the Consumer about the Categories of PI it collects, and about the Right to Opt Out.
Verifiable Consumer Request (VCR)	When the Consumer exercises their rights, they must send a Verifiable Consumer Request to the Business, which the Business can use to authenticate the Consumer, and the Business must respond in 45 days.

John Doe

jdoe@email.com | 555-123-4567

Jane Smith

jsmith@email.com | 123-555-6789

Jane Doe

Who and What is Protected (cont.)

Other CCPA areas to note:

- The business must disclose to the consumer the categories and purpose for which PI is collected
- The business has certain responsibilities in the event of a breach
- Children are considered a special category, as CCPA gives parents more control over what personal data businesses can collect from minors. Children must be affirmatively opted-in for their PI to be sold
- CCPA-compliant disclosure and notification are critical
- The law may be subject to changes as CCPA is implemented and challenged

Businesses must be able to handle verifiable consumer requests (VCRs) regarding PI; for example:

- Must segregate PI in these requests
- Requests to provide information are only for the 12 months prior to the VCR
- Must respond to a VCR within 45 days

Additionally, a business can incentivize consumers to provide their PI and permit businesses to process and sell PI. But consumers cannot be penalized if they choose not to approve use of their PI.

Penalties and Risks

Intentional violations of CCPA can result in $7,500 fine, and those lacking intent have a price tag of $2,500. In the event of a data breach, CCPA states that a business may have to compensate consumers from $100 to $750. While this amount may not seem excessive, penalties add up quickly as the fines are per consumer and per incident and there is no total fine limit, unlike with GDPR (up to 4% of annual global turnover or €20 million). A consumer does not have to show harm if their PI was breached, and they can take legal action directly against the business if their PI is breached. This is in contrast to the rest of CCPA which requires actions to be brought by the California Attorney General.

ADDITIONAL PENALTY AREAS TO BE FAMILIAR WITH:

Penalties can be assessed at the highest level based on a business' compliance efforts (or lack thereof).

Litigation (e.g. class actions) is possible.

Any reputational damage must also be counted.

The emphasis on categories in the CCPA raises some interesting metadata concerns like what the categories are, how they are defined, and how information, sources and third parties are actually categorized.

How CCPA Compares to the GDPR

The CCPA was clearly influenced by the GDPR, with some notable nuances.

The CCPA has a right to be forgotten, a right to portability and a right to access to data, which are clearly recognizable to anyone familiar with the GDPR. But there are differences too, such as explicit damages in the CCPA that can be awarded to individuals in the event of a data breach.

The CCPA does not speak of a "data subject" as the GDPR does, but rather a "consumer," meaning a natural person who is a California resident. A consumer may well be a customer but could also be an employee or a point of contact at a supplier.

Similarly, the GDPR speaks of "Data Controllers" and "Data Processors," but the CCPA just deals with "businesses" — although the spirit of distinction between the Data Controller and the Data Processor does seem to be present in the CCPA.

A noteworthy difference between the CCPA and the GDPR is a difference between metadata and data. The CCPA explicitly states that a consumer has the right to be informed of the categories of personal data, categories of sources of data and categories of third parties that a business shares personal data with.

The GDPR really only speaks about data and the need for plain language in terms of disclosures to data subjects. The emphasis on categories in the CCPA raises some interesting metadata concerns like what the categories are, how they are defined, and how information, sources and third parties are actually categorized. All of this is metadata. Of course, as noted above, consumers also have rights to actual data in the CCPA.

Personal information includes "Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities and aptitudes."

How CCPA Compares to the GDPR (cont.)

Another interesting difference is specificity about disclosures. The GDPR states that data subjects must be provided with an explanation that is clear and specific of what purposes the data will be used for. The Data Controller has some latitude in how this is to be done.

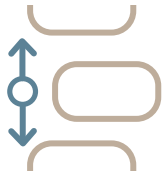
The CCPA is also more prescriptive. It states that a business which currently sells consumer data must "provide a clear and conspicuous link on the business' Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt out of the sale of the consumer's personal information."

The CCPA calls out inferences in a way that the GDPR does not. The GDPR has language about building a "profile" of a Data Subject. However, the CCPA seems to go further and includes inferences about consumers as part of personal information. Specifically, personal information includes "Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities and aptitudes."

Yet another distinction between the CCPA and GDPR is that damages can be awarded to individuals. In the GDPR, fines paid to the UK Information Commissioner's Office (ICO) can be levied for failure to comply that are four percent of global revenue or EUR 20 million (whichever is greater). The CCPA provides that in the event of a data breach, a business may have to compensate a consumer from $100 to $750. Estimates of what a data breach costs an organization have in the past previously been in the $100 to $200 range, so this could now rise significantly.

How To Prepare For CCPA

Galvanize Around Data Governance as the Foundation



Prioritize Your CCPA Compliance Efforts

Leverage Data Privacy Technology

PREPARING FOR CCPA

Galvanize Around Data Governance as the Foundation

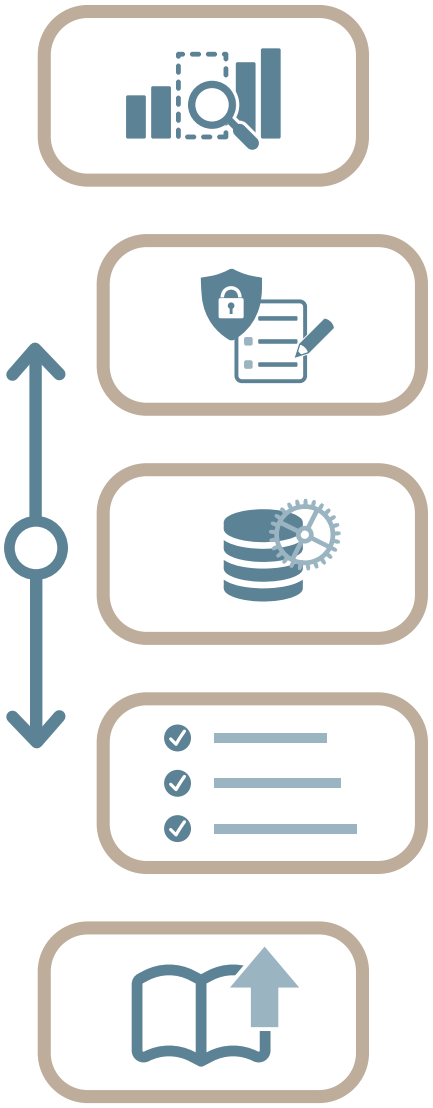
To prepare for CCPA, your organization needs to know what CCPA-sensitive data you have, where it resides and why you have it. Ultimately, the governance of data, processes, people and technology are at the heart of meeting the CCPA challenge.

To be truly effective, you should adopt an interdisciplinary effort — with engagement and collaboration across your legal counsel, chief privacy officer, information security office, key IT stakeholders and procurement or vendor management. The data governance area is the best-placed organizational unit to coordinate this collaboration, and should be tasked with partnering with the Privacy team to provide the framework for the processes, policies, organization and technologies required to manage and execute a data privacy program.

Data governance is also a good functional fit for the ongoing management, monitoring and protection controls of consumer data and consent. Although the average cost of a data breach globally in 2018 was $3.86M*, the true cost of non-compliance or the reputational damage created by either a data privacy or ethical breach could be fatal for a company.

Governance has to be involved in the projects that use the data to ensure they comply with the privacy standards. In fact, if data governance and data management capabilities have already been established at an enterprise level, you will be better positioned to comply with the CCPA and more easily adapt to other new and emerging regulations.

*2018 Cost of a Data Breach Study: Global Overview from IBM Security and Ponemon Institute



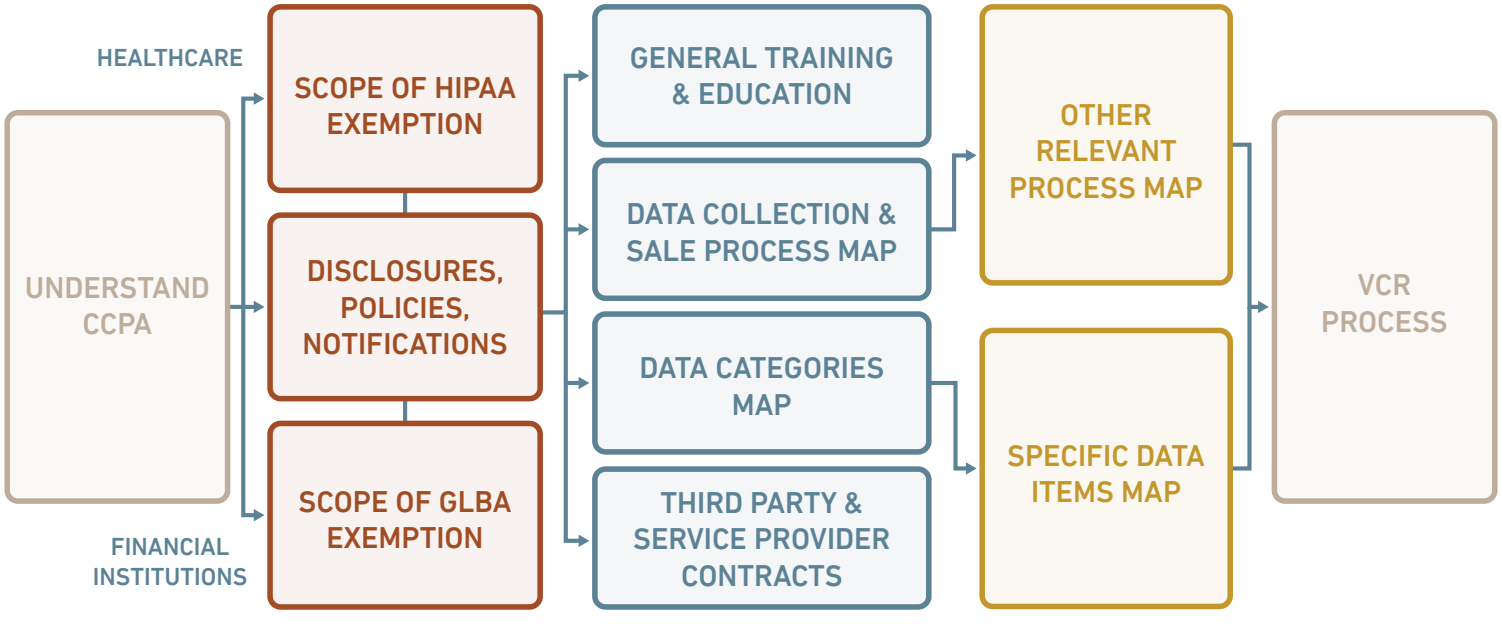
Prioritize Your CCPA Compliance Efforts

The entire scope of CCPA may not have to be solved in a single effort. There is a logical sequence of tasks (shown at a high level below in Figure 1) and your legal counsel can help decide which of these tasks can be eliminated or delayed, based on work already done, or your particular business model.

Leverage Data Privacy Technology

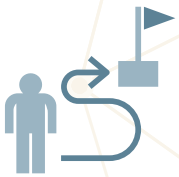
Understanding your data is critical to being able to secure and leverage it. Metadata and data lineage are critical foundational capabilities that will help you comply with these privacy regulations. Data classifications, data location, authority and access rights at the data element level all help to ensure appropriate levels of privacy are being identified and implemented. Consider taking advantage of technology solutions that help support, automate, manage and accelerate your compliance to CCPA and future privacy regulations.

Figure 1



1 *vision*

2 *purpose*



3 *picture*

4 *plan*

5 *participation*

Sustain Data Privacy

The clock is ticking on complying with CCPA and more states are in the process of developing similar laws, with potential legislation at the federal level, too. With a focus on the individual and the consumer (the most granular level of customer information), these regulatory requirements can be quite challenging.

For deeper traction and lasting impact, organizations should be prepared to initiate privacy and impact assessments for all projects and incorporate privacy by design into the development phase of projects and software enhancements. You can also foster a culture of data privacy by educating people on how to integrate privacy practices into all data management activities, data sharing and data usage.

Creating a data privacy or ethics framework is an effective and sustainable way to enable an ethical culture. The framework should call the principles and guidance around what is considered ethical (and what isn't) and could include a data privacy/ethics policy. Whether your program is "compelled" or "discretionary," the goal is to help people recognize the purpose and value of data ethics and data privacy, and enable a more ethics-aware community. The more it is embedded into the company culture, the less you need to rely on policy to drive action.

Here, at a high level, is a five-step process to help you get started in developing a data ethics framework:

1. **Vision.** Create a high-level, strategic statement of your goal.
2. **Purpose.** Share why you are executing the vision.
3. **Picture.** Help people envision what the future state looks like and the principles for attaining it.
4. **Plan.** Explain how and when the organization will get to the desired future state.
5. **Participation.** Detail who is responsible for the needed changes.

This process should align with the scope and priorities of your data privacy program. And although your vision, purpose and picture may appear lofty, aspirational or broad, your plan and who is participating will be more specific and tactical.

Ultimately, the goal is to not just have a policy, but to have a data privacy culture that uses that framework to make ethical decisions with data. The hallmarks of a robust and sustainable data privacy program should include integrated governance, internal and external privacy policies, privacy by design, continuous risk assessment, breach protocols and data privacy education and training, to name a few. To make that a reality, it's important to leverage all your organizational change management capabilities to drive awareness and adoption of a data ethics and privacy-by-design mindset.

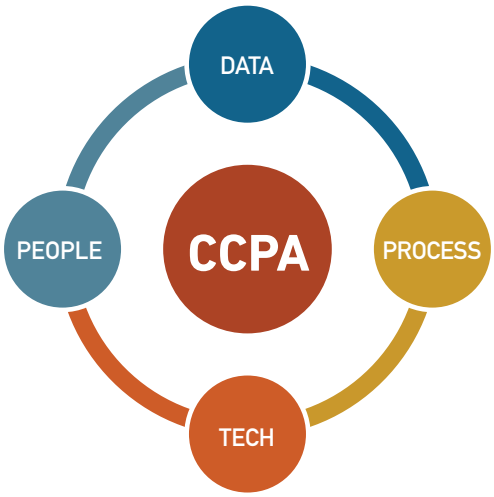
Because when it comes to data privacy, compliance is not just regulatory requirement. It's a competitive differentiator and strategic business priority.

Today's evolving data privacy landscape and increasing consumer consciousness require a response that is an ongoing program, not just a single compliance initiative.

HOW FIRST SAN FRANCISCO PARTNERS CAN HELP:

First San Francisco Partners has developed a **CCPA Playbook** to quickly put you on the road to defensible compliance. The Playbook helps organizations develop a CCPA-compliance plan in 10 days by:

- Determining where you are in terms of your organization's response to CCPA based on a breakdown of its 150 constituent elements (essentially a gap analysis)
- Identifying the tasks that have to be carried out to become CCPA-compliant
- Resolving how your organization has to configure and operate your metadata solution to support CCPA compliance
- Deriving a detailed project plan for how compliance will be reached after completion of the CCPA Playbook
- Loading pre-specified CCPA-relevant content from the Playbook into your metadata to update business glossary definitions and reference data code sets



First San Francisco Partners is dedicated to the cost-effective delivery of integrated information management solutions that enable organizations to transform their operations and achieve outstanding business success. As a premier Collibra partner since 2012, we focus on operational strategy and technical solutions for holistic data governance, metadata and implementation success. By taking a holistic approach, your organization's Collibra footprint expands to support multiple use cases, while ensuring consistent alignment to leverage maximum value out of your investment.

Collibra

HOW COLLIBRA CAN HELP:

Collibra offers a Privacy & Risk enterprise-grade platform that enables CCPA compliance and minimizes privacy-related risks. The scalable platform approach allows organizations to document, govern and collaborate around privacy policies in a centralized location, ensuring they are effectively managed across the enterprise.

Collibra's out of the box data privacy framework allows organizations to jump start CCPA implementation and achieve faster time to compliance. With Collibra Privacy & Risk, organizations can:

- Perform assessments required for CCPA
- Monitor compliance progress through easy-to-understand dashboards and reports
- Evidence compliance to regulators and other stakeholders with full audit trails
- Track and manage data exchanges with third-parties, reducing risk from vendors and partners
- Ensure personal data is kept safe and managed efficiently across its entire lifecycle
- Understand the risks inherent in personal data use within the organization and the controls to apply to mitigate them
- Support the incident response management process
- Create and maintain a process register
- Complete data inventory and mapping

With more data privacy and protection regulations expected in the next five to ten years, organizations must be prepared to adapt to the evolving regulatory environment. Collibra Privacy & Risk is designed to help organizations both adapt to CCPA and proactively build the foundation for a strong data culture that will be prepared for future regulations.

While CCPA compliance may be the catalyst for adopting a robust data privacy framework today, it is strategically important to get data privacy right in the long term. With Collibra Privacy & Risk, organizations can prioritize a strong data privacy framework that empowers users to unlock the value of their data and innovate in new and exciting ways — enhancing efficiencies, launching new products and engaging with technologies such as AI and machine learning.

DISCLAIMER

First San Francisco Partners (FSFP) is not a law firm, nor does it represent one. Therefore, neither FSFP, nor any of its employees, consultants, and sub-contractors provide legal advice on data privacy regulations (e.g. GDPR, CCPA).

FSFP expects that any enterprise that engages FSFP leverages the enterprise's Legal and Data Privacy experts, often with outside Counsel, to interpret all data privacy regulations or laws (e.g. GDPR, CCPA) as they require.

Furthermore, FSFP expects that the designated enterprise's Legal and Data Privacy expert(s) participate throughout any engagement involving FSFP to provide advice, guidance and interpretation (along with advice and/or guidance from designated outside Counsel) of the impact of all data privacy regulations or laws (e.g. GDPR, CCPA) on the enterprise.

FSFP's role is not to provide this advice and/or guidance, but rather FSFP partners with the appropriate enterprise Legal and Data Privacy experts and other key personnel in Data Governance, IT, Risk, Procurement, etc., to translate the Legal and Data Privacy experts' interpretation into operationalized practices supporting data privacy compliance.

FSFP does not guarantee compliance with any applicable laws and/or regulations (e.g. GDPR, CCPA) in any jurisdictions (e.g. California, European Union.) The expectation is that the enterprise reviews and vets the FSFP work products — including, but not limited to — content, deliverables, Readiness Assessment tools (e.g. GDPR, CCPA) — essentially all artifacts — with accredited legal experts for final opinions.

MEETING THE CCPA CHALLENGE

Now and for the Future

FIRST SAN FRANCISCO PARTNERS

info@firstsanfranciscopartners.com
www.firstsanfranciscopartners.com
1-888-612-9879

Collibra

https://www.collibra.com/demo
Request a demo
1-646-893-3042