The California Consumer Privacy Act (CCPA): Risk, revenue, and reward

The CCPA goes into effect January 1, 2020. And more U.S.-based data privacy and protection legislation is about to follow. Your risk is only one part of the equation when it comes to the impact of the CCPA. And there is another important "R" to watch – its upcoming impact to your revenue. Learn the key considerations that can enable your business to close both risk and revenue gaps, while also preparing for future legislations.

A PEGA WHITEPAPER

PEGA®

Build for Change®

Introduction

According to recent research conducted by PricewaterhouseCoopers, only about half of the U.S. businesses affected by the upcoming California Consumer Privacy Act (CCPA) expect to be compliant by the law's effective date of January, 1, 2020. And the implications for those who fail to comply could be huge. Following the General Data Protection Regulation (GDPR) that ushered in a new era of data regulations across the E.U., this new U.S. state legislation is the next major movement in the growing landscape of customer data protection and privacy. This has many U.S. businesses asking: How can we ensure that we are prepared for the arrival of CCPA?

Beginning January 1, 2020, most large organizations that do business in California will need to respond and act within 45 days to any customer who exercises their rights, including:

- The right to understand which data you have collected about them
- The right to demand that you delete that data
- The right to say no to the sale of that data to third parties

And these are just some of the rights. With the clock now ticking, many businesses are rushing to devise sound CCPA strategies and are considering the impact to compliance and risk.

But, there is often a major misconception that this state legislation is solely about risk. The reality is that risk is just one aspect of the upcoming legislation. There is an important second "R" that must be addressed - your revenue.

With the right to delete, comes a lessening of your organization's ability to leverage customer data to drive relevancy and revenue alike.

And the CCPA is likely a sign of what's to come in the U.S. – your starting line, rather than your finish line. Any solution that you deploy will not just have to address the CCPA, but all future data privacy and protection legislation from other states that will soon follow.

If you plan your strategy right, you can close all these gaps – and stay on budget.

Risk
+
Revenue
=
Reward

Disclaimer: No content herein should be considered legal advice – consult your own legal consul to determine your legal strategy.

Achieving risk readiness: Critical capabilities for CCPA compliance

At its core, the greatest challenge with CCPA is one of orchestration and auditability. And with every business' data environment, IT infrastructure, and interpretation of the legislation being different from the next, many are now waking up to the complexity of compliance. The reality is that, in order to comply, it's not a question of if you have a system to manage the CCPA – it's whether you have a system to manage the systems.

The capabilities that are key to closing the gaps for your CCPA personal data profiling compliance strategy fall under four categories: data assembly, process orchestration, acceptance strategy, and audit trail.

> It's not a question of if you have a system to manage the CCPA – it's whether you have **a system to manage the systems.**

Disclaimer: No content herein should be considered legal advice – consult your own legal consul to determine your legal strategy.

1. Data assembly

One of the first steps on your path towards a successful CCPA technology strategy is to discover and identify all of the places where individual-level customer data may be residing across your enterprise. In addition to the master data management (MDM) efforts that your business likely has under way, you may need to provide a new capability to collect and assemble this data – on demand – when a CCPA event, such as an access request, is initiated. You'll need a way to collect and assemble your customers' data for the rolling past 12 months. Your business will also need to develop a technology strategy to manage exceptions around confidential information that is covered by the legislation.

This is no small task. Consider that many businesses have had 360-degree customer view initiatives for years, that are still not complete. Now, the pressure is on as you work to provide that view directly to the customer – and this time there's a deadline (January 1, 2020).

Enabling technology

To close this gap of CCPA orchestration, you will need to establish new technology processes, both where APIs exist and even where they don't.

Yes, that old mainframe where you still keep customer data (that doesn't connect to anything,) will still play a role in your CCPA compliance strategy. But, will you have employees manually look up data and enter it into other screens by hand? For some, that's the current plan. However, there's a more effective, lower-risk solution.

a. APIs and integrations – Solutions such as Pega's Integration Wizards simplify the process of integrating with API-based data sources, guiding your administrators through the process of defining the data model from a WSDL, for example XML/JSON. Standard integration connectors are also available for SOAP, REST, and other integrations.

b. Robotic automation – Unfortunately, not every system impacted by CCPA will have a clean API or easy integration, which presents a major challenge for compliance. Rather than leaving this to time-consuming, expensive, and error-prone manual data query and duplication, best practice should be to employ robotic automation technology. These "software robots" can function both at the desktop level and the intersystem level, allowing you to distribute work across desktops, employees, and servers, so you can scale to meet your CCPA compliance needs.

c. Non-electronic and unstructured data – To make things even more challenging, the law even pertains to data that is not held electronically. Think about all that paper stored away in file cabinets, or those audio recordings of customer interactions that were collected for "quality and training purposes." This means you will likely also need to orchestrate "sneaker-net" style teams that go and fetch the required data from these locations, on demand. And with just 45 days to respond to any customer who exercises their rights, the stakes are high.

Pega's industry-leading case management technology allows you to integrate data sources, robotics, and even manual processes equally – all within a single solution.

Disclaimer: No content herein should be considered legal advice – consult your own legal consul to determine your legal strategy.

2. Acceptance strategy

The CCPA requires that your business accepts data requests through two or more designated methods, "including, at a minimum, a toll-free telephone number, and if the business maintains a website, a website address."[1]

A multi-channel requirement

This requirement means that you will need to employ a multi-channel technology strategy. Beyond offering simple self-service forms on your website, your front-line service employees must be equipped to accept these very same requests and ensure that all requests follow the same process. This is exactly the capability that Pega Customer Service™ and dynamic case management technology provides.

Identity confirmation

When it comes to ensuring each data subject's identity, the stakes are incredibly high. Even individuals authenticated on your website may pose risk. Consider how much sensitive data there is that is not typically served up on account screens. This type of data includes citizenship data, answers to personal security questions, financial information, and much more. To a hacker that has cracked the simple password the consumer forgot to change, it can be just a few clicks to log in, change the email address on record, and fraudulently request a copy of the consumer's data.

For this reason, many are advising that any change to customer data (rectification), request for access, erasure, or any other CCPA request be subject to a double opt-in style identity confirmation, and greater authentication.

Enabling technology

By employing Pega's dynamic case management capabilities, you can accept CCPA requests on any touch point. Pega's "mash-up" ability enables you to serve up data request capabilities into your existing website, maintaining the current user interface. The technology also applies the same case logic, regardless of whether the request came in via a service employee, web acceptance, email request, or any other channel.

Many businesses may wish to soon begin accepting these requests via email. To make this practice efficient, Pega's email bot capabilities can apply natural language processing (NLP) and instantly understand the intent of the communication. Through these NLP capabilities, the bot can open or assign cases, and automate the assignment throughout the organization.

[1] California Consumer Privacy Act, § 1798.104, 2018

Disclaimer: No content herein should be considered legal advice – consult your own legal consul to determine your legal strategy.

3. Process orchestration

CCPA's orchestration challenge centers upon creating new, closed-loop processes that do not yet exist in many cases. It's not just about knowing your data sources. It's about knowing how you will go about your compliance work – how you will initiate, automate, track, and report on each and every CCPA event, everywhere across your enterprise.

Some businesses may be tempted to begin their compliance journey with a simple ticketing system. But, beware that this seemingly simple solution is likely to lead to complications.

Ticketing systems can only route work. They can't actually help get the work itself done. And every manual process opens your business up to CCPA risk exposure for gaps in compliance, accuracy, and audit trail. More importantly, as new data privacy legislation rolls out, ticketing systems and manual processes will not be able to scale to accommodate the specific variations of each individual bill.

Along with accommodating for each individual bill, in certain cases, the simple acceptance processes just won't cut it. Sometimes, the system may detect risk, like if an identity could not be confidently confirmed. Other times, perhaps the request doesn't meet certain service-level agreements (SLA's) or time constraints within set processes. Some circumstances may even require legal review. And simply assigning work to individuals is fraught with risk (hint: "Thank you for your note. I'll be out of office for the next three weeks").

For best practice, you will need to have a series of progressive escalations that elevate the request to additional individuals within your organization.

Enabling technology

Pega's suite of software offerings can help you tackle CCPA compliance head-on. By employing Pega's dynamic case management technology, your business can rapidly configure how your processes should flow, along with SLAs, and escalations to make sure the job gets done. The technology enables you to establish the necessary workflows without software coding. This no-code approach will help you provide the right information as demanded by the legislation, while also offering transparency into your business processes, steps you have taken, and your adherence to protocol.

Your CCPA challenge is just the beginning: Gear up for future legislations

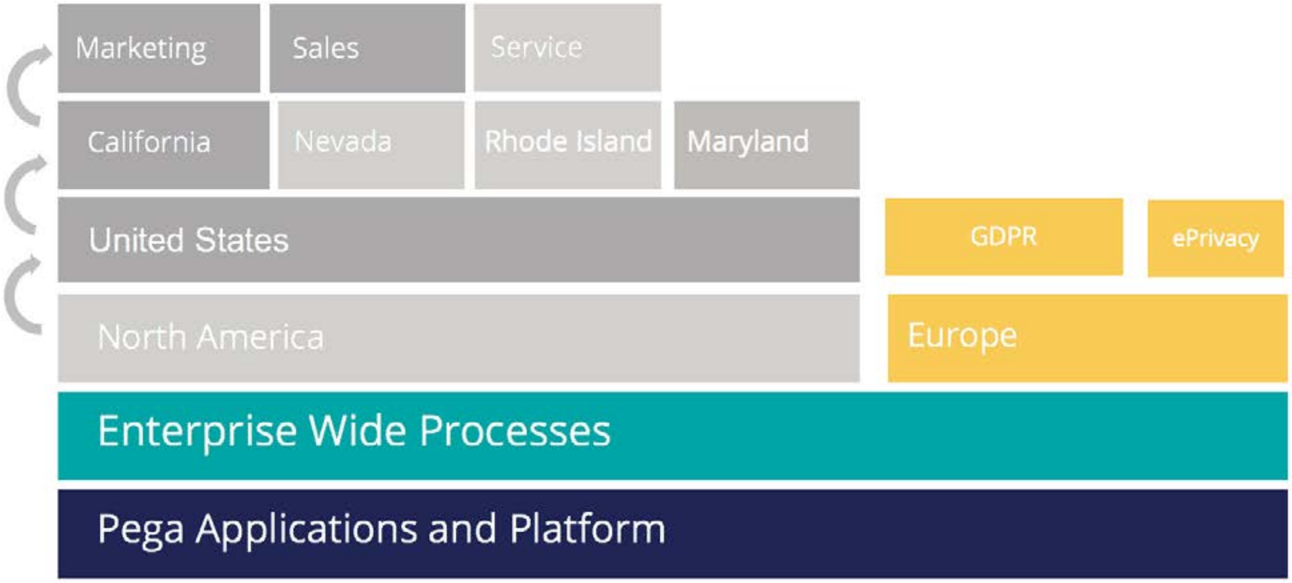
CCPA is likely to be just the first domino to fall in the U.S landscape of customer data privacy and protection. Legislation from many other states could be coming soon. Already, states including Hawaii, Massachusetts, Maryland, Mississippi, Nevada, North Dakota, New Mexico, New York, Rhode Island, and Washington are introducing proposed bills to the Senate – each with their own set of specific terms and conditions. These terms include differences in scope, definitions, consumer rights, penalties, and disclosure obligations. Your business needs a solution that can handle all of the permutations that will follow – and at scale.

A ticketing system simply won't cut it. With potentially massive risk and revenue loss, the time to get your head around these future legislations is now.

Disclaimer: No content herein should be considered legal advice – consult your own legal consul to determine your legal strategy.

Your CCPA challenge is just the beginning: Gear up for future legislations continued...

Only Pega can empower you with a future-proof system. Rather than establishing duplicate, disconnected strategies for each process and regulation – which will be impossible to scale – you can leverage Pega's Situational Layer Cake Architecture^{TM}. This patented capability addresses the challenges of a multi-dimensional hierarchy. It enables your business to efficiently manage compliance and process differences in ways that facilitate reuse and rein in the complexity.



By allowing our clients to differentiate, specialize, and reuse business applications, Pega's situational layer cake can dramatically accelerate the time to value to meet the demands for future legislations on customer data privacy and protection.

Disclaimer: No content herein should be considered legal advice – consult your own legal consul to determine your legal strategy.

4. Audit trail

The bottom line when it comes to all things CCPA? Prove it and track everything. It's not just about the execution. It's about providing evidence of compliance with each of the CCPA's challenging sections.

Which steps have you taken? How exactly did you provide each individual with the resolution they demanded? How long did it take? How did you validate each data subject's identity at the time of the CCPA request? Which safeguards did you put in place while their data was in motion?

And how do you plan to track not just your policies, but when those policies were changed? And by whom?

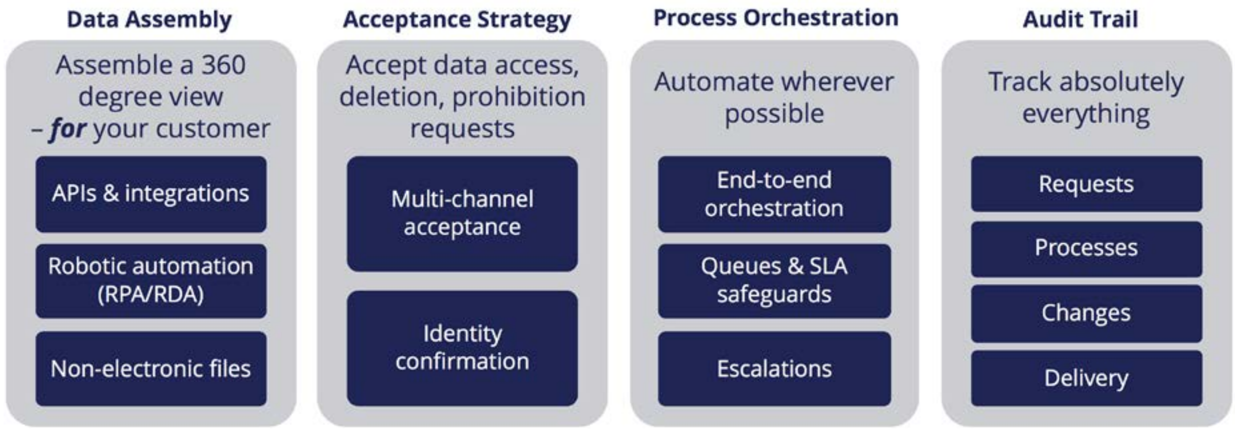
Enabling technology

With so much on the line, your accountability strategy cannot be an afterthought. It has to be in the very bedrock of your processes. Pega's powerful dynamic case management solutions include the out-of-the-box ability to track everything, across each of your data movements and CCPA processes. With extensive logging and tracking, this includes your ability to play back not only which interactions occurred, but also which customer data supported those decisions at each step.

And for additional granularity, capabilities such as Pega Business Intelligence Exchange™ (BIX) can provide the ability to automate the selection and extraction of data into external files (in XML or comma-delimited format), or a relational database.

By incorporating these core capabilities of data assembly, process orchestration, acceptance strategy, and audit trail into a holistic strategy, your business can establish **the system to manage the systems** – and help you close your CCPA compliance gaps.

Illustration: Core competencies for CCPA risk-readiness



Data Assembly

Assemble a 360 degree view – ***for*** your customer

- APIs & integrations
- Robotic automation (RPA/RDA)
- Non-electronic files

Acceptance Strategy

Accept data access, deletion, prohibition requests

- Multi-channel acceptance
- Identity confirmation

Process Orchestration

Automate wherever possible

- End-to-end orchestration
- Queues & SLA safeguards
- Escalations

Audit Trail

Track absolutely everything

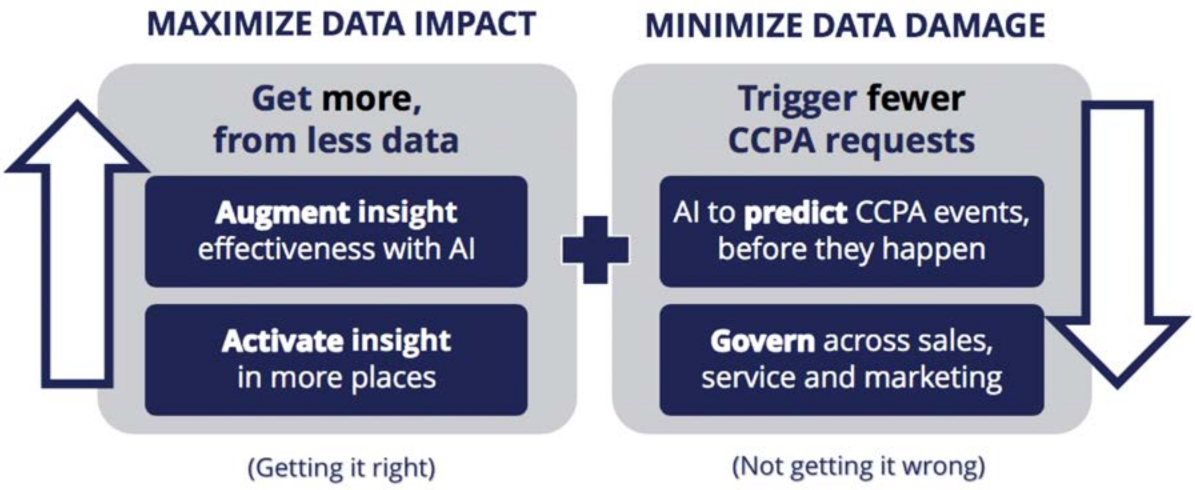
- Requests
- Processes
- Changes
- Delivery

Disclaimer: No content herein should be considered legal advice – consult your own legal consul to determine your legal strategy.

Achieving revenue readiness: The CCPA's looming impact to your bottom line

Many may mistake the CCPA to be simply an issue of compliance or risk. The wake-up call comes when businesses finally look close enough to realize that CCPA legislation is not just a problem of risk – but also revenue. And it's much more than the potential $7,500 fine per user violation that comes with failure to comply.

Your revenue exposure will fall into two categories: Maximizing data impact and minimizing data damage.


MAXIMIZE DATA IMPACT
MINIMIZE DATA DAMAGE
Get more, from less data
Augment insight effectiveness with AI
Activate insight in more places
Trigger fewer CCPA requests
AI to predict CCPA events, before they happen
Govern across sales, service and marketing
(Getting it right)
(Not getting it wrong)

1. Maximize data impact: Extracting greater results from less customer data

Consider that for more than a decade, the demand for data-driven decisions has exploded. Businesses of all shapes and sizes have established proficient practices to dissect and analyze customer data, for the purpose of better understanding customers and influencing customer lifetime value (CLV).

Of course, the fuel for any business' insight engine is customer data. Over the years, you've acquired customer data not just from individuals, but also from third parties, in the hope of gleaning greater insight into each individual's needs and behaviors.

Now, a new reality is about to sink in: Beginning January 1, 2020, nearly every large organization that does business in California will have to make do with less data to work with. To produce the same results as today with less customer data, businesses will need to improve their insight-driven practices and achieve greater accuracy.

This will mean that you need to maximize the value of the customer data that you do have available, by using more insight in places than ever before.

Disclaimer: No content herein should be considered legal advice – consult your own legal consul to determine your legal strategy.

2. Minimize data damage: Limiting the triggering of CCPA requests

Not only will you have to learn how to do more with less - you'll also have to develop a new competency around making sure you don't get it wrong. Every "less-relevant" interaction brings your organization one step closer to a CCPA- driven complaint. According to a Pega consumer survey, robocalls, irrelevant marketing, high marketing frequency, and poor customer service interactions are among the likely triggers for a customer initiating an erasure request.[2]

Interactions like these lead an individual to question why they have been treated in a certain way (by sales, service, and especially marketing), and will only increase the probability of a data access or erasure challenge. It will often be your own actions as a business that will drive the data depletion – and costs – that come with each CCPA-driven event.

The problem is that, traditionally, marketing offers have largely been regarded by marketers on a scale of being either highly relevant or potentially relevant, with varying degrees in-between. Any given offer could potentially hold the opportunity to drive revenue, so up until now, there was very little risk in getting the offer wrong.

Consider that the average marketing campaign yields just a 1-2% response rate. Come CCPA, these irrelevant offers could come with a cost. Sometimes, the next best action is to send no offer at all. The businesses that will best rise to this challenge will reframe their approach to marketing. They will establish new processes to ensure that potentially irrelevant content and treatments are held back – and these decisions will be made in real time.

These two aspects of augmenting insight effectiveness, while at the same time restricting communications, may seem to be at odds with each other. They will, however, become critical elements of your new strategy on your road to revenue success in the era of the CCPA.

Enabling technology

The key for CCPA revenue-readiness will lie in the decisions that you make. The relief comes when you realize that with the right strategy, you can achieve risk-readiness and revenue-readiness in one fell swoop. The same technology that would help mitigate CCPA risk can also set you up to exceed your revenue targets.

And Pega offers technology that can help you do just that. With powerful AI-driven analytics for determining the next best action for every individual – in real time – our software understands CLV. It helps you weigh the risk and the reward of every potential action and empowers your business to make the most of the data you have. And of course, it works seamlessly with all of your existing infrastructure.

[2] Pegasystems, "GDPR: Show me the data," 2017, retrieved from: https://www.pega.com/gdpr-survey

Conclusion: Risk, revenue, and reward

CCPA is coming. For those businesses that can devise an effective strategy for risk and revenue readiness, as well as gear up for future legislations, there can be great reward. While your competitors may miss the big picture and devote their efforts (and budget) to systems that can only assist with compliance, your business can use this moment as an opportunity. Get it right the first time. Determine the appropriate requirements and implement an infrastructure that solves orchestration challenges for both risk and revenue. Put in place a future-proofed system that can handle not just the CCPA, but all the legislations that follow.

By remembering the two R's – risk and revenue – you can prepare a strategy for true success. If you do, the rewards will follow.

To learn more and get started today, visit **pega.com/ccpa**

Disclaimer: No content herein should be considered legal advice – consult your own legal consul to determine your legal strategy.

We are Pegasystems, the leader in software for customer engagement and operational excellence. Our adaptive, cloud-architected software – built on the unified Pega Platform™ – empowers people to rapidly deploy and easily change applications to meet strategic business needs. Over our 35-year history, we've delivered award-winning capabilities in CRM and digital process automation (DPA), powered by advanced artificial intelligence and robotic automation, to help the world's leading brands achieve breakthrough business results.

For more information, please visit us at **www.pega.com**