California Consumer Privacy Act of 2018 (CCPA)
California Privacy Rights Act (CPRA)
External FAQs – Updated January 2021

This document is a broad overview of the CCPA and CPRA and does not provide legal advice. We urge you to consult with your own legal counsel to discuss the requirements applicable to your specific situation.

Contents

The California Consumer Privacy Act (CCPA)

1. What is the CCPA?

The California Consumer Privacy Act of 2018 (CCPA) is a new law designed to protect the personal information of California residents. It is a first-of-its kind state law in the United States that grants individuals new rights to understand and control how their information is used, shared, or sold by companies operating in California.

The law became effective **January 1, 2020**.

2. Who is subject to the CCPA?

Companies, like Mastercard, that collect personal information of California residents ("consumers") and have annual revenues of over $25 million will be subject to the law. Additional companies in scope include those that alone or in combination annually buy, receive, sell or share for commercial purposes the personal information of 50,000 or more consumers, households, or devices; and those that derive 50% or more of their annual revenue from selling consumers' personal information.

3. Is the CCPA really just an expansion of GDPR in the United States?

No. While there are some common elements between the CCPA and Europe's General Data Protection Regulation ("GDPR"), the two are not a one-for-one match. For example, while both laws grant consumers a right of access to and deletion of their personal information, those rights are not identical. This means that companies who comply with the GDPR do not automatically comply with the CCPA. For questions regarding common requirements between the GDPR and CCPA, please contact PrivacyAndDataProtection@mastercard.com or any member of the Privacy and Data Protection team.

4. What is Mastercard doing to comply with the CCPA?

Mastercard assessed the changes required to achieve compliance with the CCPA by conducting privacy design sessions with each of our business lines and functions. Mastercard implemented controls to satisfy the CCPA requirements, leveraging those that were put in place to comply with GDPR where appropriate, and continues to enhance and build upon these controls. Mastercard also accounted for any necessary alterations to our products, platforms, or services in light of the new law.

Definition of Personal Information

5. What data is considered personal information under the CCPA?

Under the CCPA, **personal information** is broadly defined and includes any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked directly or indirectly with a particular consumer or household. Some examples of personal information identified in the CCPA include:

- any persistent identifier
- geolocation data
- biometric information
- profiles created from inferences derived from other types of information.

Personal information does not include information that is 'de-identified,' or 'aggregate consumer information.' Personal information also does not include 'publicly available' information that is from federal, state, or local government records, such as professional licenses and public real estate/property records.

6. Is employee personal information in scope?

Under the original text of the law, employee personal information was within scope and subject to all CCPA requirements. However, an amendment passed in October 2019 took employee information out of scope from all but two of the CCPA's requirements until 2021.

As a result, the majority of the CCPA's requirements will not apply to the following personal information until January 1, 2021:

- Personal information about a job applicant, employee, director, officer, medical staff member or contractor to the extent that the personal information is collected and used solely within the context of that individual's current and/or former role as such;
- Emergency contact information of that individual;
- Personal information necessary to administer benefits for another natural person relating to that individual.

This 1-year exemption does not apply to the CCPA's notice requirements or private right of action. Therefore, employees still have the right to bring civil actions for data security breaches affecting the personal information maintained by their employers.

The California Privacy Rights Act **extends the exemption for employee information to January 1, 2023** (see response to FAQ 16). If the exemption is not made permanent by that date, employee information will be within scope of the CPRA.

7. Is business-to-business personal information in scope?

Under the original text of the law, personal information of business contacts (collected and used in the context of a business-to-business or "B2B" relationship) was within scope and subject to all CCPA requirements. However, an amendment passed in October 2019 took certain B2B personal information out of scope from some, but not all, of CCPA's requirements until 2021.

As a result, certain sections of the CCPA will not apply to personal information collected about a consumer through business-to-business (B2B) communications (written or verbal) or transactions where:

- the consumer is acting as an employee, owner, director, medical staff member or contractor (collectively, "employee") of a company, partnership, sole proprietorship, nonprofit or government agency; and
- the personal information is collected and used solely within the context of conducting B2B due diligence or providing or receiving a B2B product or service.

This personal information will be exempt from the CCPA's requirements to provide notice, and to satisfy access, deletion, and portability requests until January 1, 2021.

The California Privacy Rights Act **extends the exemption for B2B information to January 1, 2023** (see response to FAQ 16). If the exemption is not made permanent by that date, B2B information will be within scope of the CPRA.

8. What if the personal information is already regulated under existing federal law?

The CCPA provides for certain exemptions where existing federal law applies. For financial institutions, personal information that is collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act and its implementing regulations, or the California Financial Information Privacy Act is exempted from most of the CCPA's requirements except those concerning ensuring reasonable security is in place around the data.

9. Does the CCPA apply to physical documents?

Yes, the CCPA applies to personal information in any format. That means not just data in digital formats, but also hard copies.

Individuals' Rights

10. What kinds of rights are granted to individuals under the CCPA?

The CCPA grants expanded choice and control to California residents over how their personal information is handled by businesses who operate in the state. In particular, they are granted a:

- **Right to know** what categories of personal information is collected about them, sold or disclosed;
- **Right to opt-out** from the sale of that information;
- **Right to request deletion** of personal information subject to a few exceptions;
- **Right to access** that personal information, free of charge, in a portable and readily useable format; and
- **Right to equal service and price**, even if they exercise their privacy rights ("non-discrimination").

When a California resident approaches a covered business to exercise any one of these rights, the business has forty-five (45) days to respond under the CCPA.

Penalties

11. What happens if the CCPA is violated?

The CCPA is enforced by the Attorney General of California, who has the authority to impose civil penalties of up to **$7,500 per violation** for companies that intentionally violate the CCPA rules. California residents have a private right to sue companies under the CCPA only if their personal information is subject to a data breach and certain requirements are met.

Compliance with the CCPA

12. How does Mastercard demonstrate its compliance with the CCPA?

Since it was passed in June 2018, Mastercard has viewed the CCPA as another opportunity to review and strengthen our practices – which we regularly do as a matter of course – and to give individuals clear, simple methods for exercising their rights under the law. For example, as of January 1, 2020, California residents are able to make use of Mastercard's **My Data** portal to access, correct or delete their personal information.

We recognize we play a key role in the payment ecosystem so we are working closely with customers, partners and vendors to help them understand the requirements and how best to comply. We also updated our websites and our privacy notices to reflect necessary changes required as a result of the CCPA and will continue make any additional changes as required by the CCPA implementing regulations once they have been finalized by the California Attorney General's Office.

13. Will the law change in 2021?

The text of the CCPA has been final since October 2019 and can only be further amended through the statutory legislative processes provided by California law.

However, the CCPA also required the California Attorney General's Office to promulgate implementing regulations by June 30, 2020, to further elaborate and shape how this new law will be applied. Mastercard reviewed the multiple drafts of the implementing regulations, which were released over the course of nine months. Though delayed, the final regulations have now been approved and become enforceable in October 2020.

Notwithstanding the issuance of final regulations, the Attorney General has subsequently proposed (and may continue to propose) modifications to the regulations. We will continue to monitor development and assess their impact on Mastercard.

The California Privacy Rights Act (CPRA)

14. What is the CPRA and how does it impact the CCPA?

In September 2019, Alistair Mactaggart, one of the original drafters of the ballot initiative that created the CCPA, filed a new ballot initiative to create the California Privacy Rights Act (CPRA). The CPRA is an omnibus data protection law that builds on the rights provided under the CCPA and more closely aligns with the GDPR.

On November 3rd, the **CPRA was approved** by California voters. It will **replace** the CCPA and become wholly operational on January 1, 2023. The CCPA would remain in full force and effect until the CPRA becomes operational.

15. Does the CPRA impose new requirements?

The CPRA expands on the rights the CCPA currently provides to California residents ("consumers"), and requires companies to provide consumers with additional controls over how their personal information is handled in the following ways:

- Right to request that a business **correct inaccurate personal information** that is maintained by a business
- Right to **limit use and disclosure of Sensitive Personal Information**, which includes biometrics, geolocation, racial and ethnic origin and credit card numbers if together with the security code or password
- Right to **access and opt-out with respect to profiling**, which refers to the use of an automated process to evaluate personal information to make decisions or predictions about an individual
- Right to **opt out of** data sale or **sharing**, which extends the consumer opt-out right to cover "sharing" of personal information, a new definition that includes the disclosure of personal information to a third party for purposes of "**cross-context behavioral advertising**."

16. What are other key changes from the CCPA?

The CPRA makes significant changes to both the structure and operation of the CCPA in the following ways:

- **Enforcement:** The CPRA creates a new agency, the California Privacy Protection Agency (CPPA) to implement and enforce the CPRA. The CPPA would be the first agency of its kind that is dedicated exclusively to privacy. It would have subpoena and audit powers and would have authority to impose fines up to $2,500 per violation of the CPRA, and $7,500 per violation if intentional.

- **Breach:** The CCPA provides a private right of action to consumers in the event of a breach of their nonencrypted, nonredacted personal information. The CPRA expands the right by allowing consumers to also bring suit for unauthorized access or disclosure of their email address together with the password or security question/answer.
- **Employee & B2B Data**: The current text of the CCPA excludes employee information and business-to-business communications, but the exemption sunsets on January 1, 2021. The CPRA extends both exemptions through January 1, 2023.
- **Security & Integrity Exemption:** The CPRA expands the exemption for uses of data that allow businesses to protect the security and integrity of its networks and systems, and to guard against fraudulent uses of personal information.

17. Is Mastercard preparing for the CPRA?

Yes. As we prepare for the CPRA, we will build upon the work accomplished to implement the CCPA. In particular, we will continue to leverage our My Data Portal to provide consumers with expanded privacy rights. In addition, our new Privacy by Design tool will allow us to conduct privacy risk assessments in a collaborative and efficient manner across our business teams. We are currently analyzing the CPRA and engaging with business teams to identify incremental changes required to our products, services as well as our business processes and technologies.

18. What happens next?

Now that the CPRA has become law, it will replace the CCPA, and apply to information collected by businesses after January 1, 2022. Several provisions of the CPRA are open-ended and left to be further developed by implementing regulations issued by the California Privacy Protection Agency. The **CCPA remains in full force and effect** until the CPRA becomes wholly operational on January 1, 2023.

19. Further questions?

If you have any additional questions or comments regarding the CCPA or CPRA and how they may affect Mastercard or your business line(s), please reach out to any member of the Privacy and Data Protection team at PrivacyAndDataProtection@mastercard.com, and for further information on Mastercard's Global Privacy Program, see our Privacy Center.

We also welcome the opportunity to partner with our customers, partners, and others to discuss potential implications on our industry, and practical solutions to get into compliance.

Last updated: January 27, 2021