HERZOG

HERZOG FOX & NEEMAN

The CPRA v. the CCPA Playbook

What Companies Must Do to Comply with the New Privacy Act in California

September 2022

Introduction

California's updated privacy act - the California Privacy Rights Act **("CPRA")** - enters into force on 1 January 2023.

The **CPRA** amends the current privacy law in California (the California Consumer Privacy Act **("CCPA")**) and brings the California data protection standards closer to the one companies may be familiar with from the European Data Protection Regulation **("GDPR")**. However, these laws vary in many aspects (see our detailed comparative analysis between these laws and the additional recent privacy laws enacted in a number of US states). Companies that have prepared for the CCPA and implemented the applicable requirements in their data processing activities, will have to review their practices, procedures and policies, and further adjust them to meet the amended CPRA's requirements.

Failing to comply with the provisions of the CPRA can result in fines up to **$2,500 for each violation**, and up to **$7,500** in case the violation is concerning the personal information of a minor under the age of 16. The California Attorney General has already initiated significant enforcement measures against violators of the California privacy laws, **and not complying with the CPRA poses a major risk to companies doing business online in California.**

To assist with understanding the updated requirements, we are pleased to present our **CCPA v. CPRA** Playbook, which provides a general overview of the changes presented by the CCPA under each of the following categories, and the **practical** steps that companies, which have prepared for the CCPA, must take in order to comply

Table of Content

Scope of Personal Data

What Changed?

The CCPA temporarily exempted **employee** and **business-to business** personal data from its scope. The CPRA extended the exemption until 1 January 2023. Consequently, the privacy related requirements will now apply to this data, similarly to consumers' data, as well.

What Should You Do?

- Companies must review their entire data processing activities, and apply the policies, procedures and data processing contracts to **employee and business-to-business personal** data as well. The initial steps and requirements are detailed in our CCPA playbook, which are supplemented by the CPRA requirements in this document.

Threshold for Applicability

What Changed?

One significant change introduced by the CPRA is the threshold for the application of the law. The CPRA will apply to all entities that conduct business in California **("Business")**, and at least one of the following thresholds apply:

- The entity has annual gross revenues in excess of $25 million;
- The entity derives fifty (50) present or more of its annual revenues from selling the personal information of consumers;
- The entity handles the personal information of **100,000 or more consumers or households**; or
- The entity had chosen voluntarily to be bound by the CPRA and the California Privacy Protection Agency.

What Should You Do?

- Companies should **map their data processing activities** in order to determine whether their activities expose them to the updated material scope of the CPRA.
- Companies should determine whether **as part of their strategic data protection planning**, they wish to voluntarily be bound be the CPRA.

What Changed?

Another change implemented by the CPRA **concerns the rights granted to data subjects**. In addition to the current rights under the CCPA, the CPRA takes a leap towards the GDPR and grants data subjects the following rights:

- **Deletion:** The CCPA had granted data subjects the right to request to delete their personal information. However, Businesses must **notify** all third parties to whom the Business was sold/shared such personal information to delete the data subject's personal information, unless this proves as impossible or involves disproportionate effort.
- **Correction:** Data subjects are allowed to correct inaccuracies in their personal information.
- **Object to Sale or Share:** Data subjects are allowed to object to the sharing of their personal information for behavioral advertising purposes.
- **Object to Profiling and Automated Decision Making:** Data subjects can ask companies to cease from using automated decision making and profiling.
- **Data Portability:** Businesses must transfer personal information to another organization, to the extent requested by the data subject and if technically feasible.

Sensitive Personal Information: The CPRA also had added a definition of "Sensitive Personal Information", which includes social security number; passport number; financial account credentials; precise geolocation; racial, ethnic or religious information; contents of data subjects' emails (with other entities other than the Business); and genetic data. Publically available information, as defined under the CCPA is not considered Sensitive Personal Information.

The CPRA includes various provisions that specifically apply to Sensitive Personal Information, including:

- **The Right to Limit Use and Disclosure of Sensitive Personal Information:** Data subjects are allowed to request companies to limit the use or to stop using their Sensitive Personal Information.

What Should You Do?

- **Companies should update their internal practices and procedures** to cover the new rights granted under the CPRA. Companies must update their privacy policies to provide **details to data subjects regarding their new rights**, including a "Do not share my personal information" link on the company's website and privacy notices.
- Companies must **provide data subjects the option to object to the use and disclosure** of their Sensitive Personal Information by providing a "Limit the use of my sensitive personal information" link on the company's website.
- Companies must keep a **confidential record** of all **deletion requests** to prevent the personal information to comply with the CPRA.
- Companies should review whether they are using **automated decision making** or **profiling** to evaluate certain personal aspects relating to their data subjects.

What Changed?

The CPRA introduced a few new **privacy principles** that were not included in the CCPA, including:

- **Purpose Limitation:** Businesses can only use personal information for the purpose for which it was originally collected.
- **Storage Limitation:** Businesses should destroy or delete personal information once the data had been used for its collected purpose.
- **Security Measures:** All Businesses must implement appropriate security measures, in accordance with the sensitivity of the personal information and the harm that could be resulted due to unauthorized access.
- **Audits and Risk Assessment:** Businesses whose processing presents a significant risk to data subjects' privacy or security must conduct an annual cybersecurity audit. Moreover, these Businesses should submit to the California Privacy Protection Agency an annual risk assessment with respect to their processing of personal information.

What Should You Do?

- Companies should **map their data processing activities** in order to determine whether personal information is used only for the purpose for which it was originally collected.
- Companies should review, update and maintain **their internal policies and procedures which govern the retention and destruction** of personal information.
- Companies which process Sensitive Personal Information or that their processing presents significant risk to data subject's privacy **must conduct an annual cybersecurity audit.**

What Changed?

Under the CPRA, Businesses will be required to enter into **written contractual agreements** with entities who receive personal information from the Business. This requirement will also apply with respect to the newly defined **"Contractors"** under the CPRA and other Service Providers.

Consequently, such entities would need to **bind their subcontractors to the same written terms**, and **notify the Business of any engagement with a new subcontractor**. In these agreements, the Business' partners will need to adhere to the CPRA's requirements, including the following:

- Retain, use, or disclose personal information only for business purposes;
- Refrain from selling the personal information;
- Refrain from retaining, using, or disclosing the information outside of the direct business relationship between the person and the business;
  Certify understanding of and compliance with the contractual terms; Notify the Business if it cannot meet its obligations under the CPRA;
- Grant the Business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.
- Restriction on combination of personal information (including separate retention of data obtained for advertising and marketing purposes from other data);
- Duty to monitor compliance; and
- Ensure sub-processors are required to the same contractual terms.

What Should You Do?

› Companies should **review and update their engagements** with their service providers and other recipients of personal data, and to **implement the applicable and adequate contractual guarantees** as required under the CPRA.

Cocnclusion

The CPRA presents an important regulatory development for entities that conduct business in connection with personal data of California residents – companies should follow the recommendations set out above and assess how the CPRA apply to their data processing activities. Feel free to contact us if you have any questions regarding the new law and its potential effects on your company's compliance efforts.

Herzog Technology & Regulation Department

Herzog's **Technology & eCommerce Regulation Department** is a recognized market leader in its field. The team is led by domain experts who possess a unique set of vital, **interdisciplinary** and **global** regulatory advisory skills, and are uniquely positioned to advise a range of clients, including leading multinational technology companies as well as start-ups and disruptive technologies vendors, on applicable regulatory and compliance considerations in numerous technological areas.

We understand that the **regulatory exposure** and scope of required **attention** of almost any company operating in the **digital and technological sphere** are much wider than one specific jurisdiction or legal discipline. As our clients are often on the forefront of this ever-evolving landscape, we further understand the impact of industry trends and compliance demands on our clients' businesses. Therefore, our team possesses in-depth knowledge of the increasing volume of regulations, enforcement actions, legislative and industry trends in a **myriad of jurisdictions, digital platforms** and leading **self-regulatory** guidelines. This enables our team to offer **practical, holistic** and **comprehensive** solutions for complex situations often presented by innovative technologies and disruptive business solutions, providing "hands-on" support to our clients on the strategic, corporate and operational aspects of their business, with the aim of mitigating our clients' legal and business risks.

Regulation of **personal data** has been dramatically expanding on a global basis. Companies processing data of hundreds of millions of data subjects as well as small strat-ups-all are required to spend significant resources on understanding and implementing the constantly evolving legal challenges. Our **Privacy & Data Protection** team guides our clients on all matters relating to their data usage and assist them in navigating the numerous data protection regimes, in all the jurisdictions in which they operate.

This document does not constitute an exhaustive legal opinion or regulatory overview of any and all applicable regulatory requirements regarding the topics addressed by it, but rather, only outlines the key issues arising from the regulatory requirements. Since we are not licensed to practice law outside of Israel, this document is intended to provide only a general background regarding this matter. This document should not be regarded as setting out binding legal advice, but rather a general overview which is based on our understanding of the practical interpretation of the applicable laws, regulations and industry guidelines.

Ariel Yosefi | Partner
Head of Technology & eCommerce Regulation
yosefia@herzoglaw.co.il

Eden Lang | Associate
Technology & eCommerce Regulation
lange@herzoglaw.co.il

Mai Arlowski | Intern
Technology & eCommerce Regulation
arlowskim@herzoglaw.co.il

Ido Manor | Partner
Technology & eCommerce Regulation
manori@herzoglaw.co.il

Dima Zalyalyeyev | Associate
Technology & eCommerce Regulation
zalyalyeyevd@herzoglaw.co.il

Shlomo Friedman | Intern
Technology & eCommerce Regulation
friedmans@herzoglaw.co.il

Ruly Ber | Partner
Technology & eCommerce Regulation
berr@herzoglaw.co.il

On Dvori | Associate
Technology & eCommerce Regulation
dvorio@herzoglaw.co.il

Liron Adar | Intern
Technology & eCommerce Regulation
adarl@herzoglaw.co.il

Dan Shalev | Partner
Technology & eCommerce Regulation
shalevd@herzoglaw.co.il

Kevin David Gampel | Associate
Technology & eCommerce Regulation
gampelk@herzoglaw.co.il

Moran Bergman | Associate
Technology & eCommerce Regulation
bergmanm@herzoglaw.co.il

Or Noy | Associate
Technology & eCommerce Regulation
noyo@herzoglaw.co.il