

CCPA Compliance Playbook

For GDPR Compliant Companies

The [California Consumer Privacy Act of 2018](#) ("CCPA"), will take effect on January 1, 2020. The overall aim of the CCPA is to grant consumers greater control over the use of their personal information online, and similarly to the European General Data Protection Regulation ("GDPR"), it will have an **extra-territorial reach**.

The purpose of this document is for it to be used as an index, or a "playbook" for building and maintaining a privacy compliance working plan. The "playbook" outlines the key requirements, which apply to **companies that have already undergone the comprehensive process in order to comply with the GDPR** (see our related [GDPR Playbook](#)), and in addition, it highlights the **key steps that should be taken in reviewing and updating the GDPR related procedures, including to align them with the additional and somewhat different requirements set under the CCPA**.

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. We will be happy to provide further guidance on their applicability and the specific requirements with respect to each of the topics outlined below.

Legend

For ease of reference, the guidelines are marked with the following icons:



Perform mapping, review and analyze process.



Be aware of requirements and make internal decisions in order to comply.



Train, assign or appoint relevant stakeholders in the company.



Document in the company's internal procedures.



Implement in contracts and customer-facing policies.

Scope of applicability



Map the company's data processing activities in order to **determine whether such activities expose it to the territorial scope under the CCPA**. The CCPA applies to any organization conducting business in California that either:

- has **annual gross revenues in excess of \$25 million**, or
- **annually handles the personal information of 50,000 or more consumers, households, or devices**, or
- otherwise **derives 50 percent or more of its annual revenues from selling the personal information of consumers**.



Map the company's data processing activities in order to **determine whether such activities expose it to the material scope set under the CCPA**. The definition of "personal information" under the CCPA is **not completely identical to that under the GDPR**.



Review the **possible applicability of other relevant Federal privacy laws** (such as the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act or the Health Insurance Portability and Accountability Act), that would **exempt your company from most of the CCPA's provisions**.



Determine whether, as part of your company's **strategic data protection planning**, your company intends to adopt a **global compliance policy** that would meet the highest regulatory standard "across the board", or whether it would be more appropriate to implement **various and necessary procedures to specific jurisdictions**.

Data subjects rights



Review your privacy policy/notices and update it/them in order to meet each of the new requirements under the CCPA, including the following (some of which are currently not included in the GDPR-based privacy policies or are implemented differently):

- Detailed information on the **use and processing of the personal information collected by the company**;
- Providing notice of the **CCPA's right to access personal information**;
- Providing notice of the **CCPA's right to delete personal information**;
- Include a **'Do not sell my personal information' link** on the company's websites and privacy notices;
- Describe the **information that the company shares with service providers**;
- Describe the **types of entities to whom the company sells information**; and
- Include **two or more designated methods for submitting information requests**, including as a minimum, a toll-free number and a website address.

-  Update your company's **Right of Access Procedure** in order to reflect the CCPA's specific requirements (both material and procedural) and include standard communications that can be sent to data subjects who make access requests.

-  Update your company's **Right to Be Forgotten / Deletion Procedure** in order to reflect the CCPA's specific requirements (both material and procedural), as well as **different exemptions** that are provided in the GDPR. Including standard communications that can be sent to data subjects who make access requests.


-  Update your company's **Rights to Restrict and Object Processing Procedures** in order to reflect the CCPA's specific requirements (both material and procedural), including with respect to the **right to opt-out from having information of data subjects sold** and the requirement for **opt-in, in the case of information concerning minors**.

-  Put in place an appropriate policy for managing **requests** by data subjects who exercise their **right to equal service and price** under the CCPA.



-  Review your company's **pricing policies, marketing approach and practices** in order to ensure that they **do not discriminate whether or not a person exercises his/her rights, including price discrimination for opt-out of the sale of a person's information to third parties**.

-  Ensure your company's websites include information on **two or more designated methods for submitting information requests** and a **"Do Not Sell My Personal Information"** link.




Service provider agreements

-  Update your **Data Processing Agreements** in order to apply the relevant CCPA requirements for applicable service providers with whom the company shares personal information on Californians.

Security and data breach notification

-  Review and update the company's **information security procedures**.
-  Update your company's internal data breach procedures in order to comply with **California's regulatory data breach notification requirements**, including with respect to incident identification and response plans. In addition, update your company's internal guidelines in order to assess the need to provide notifications to Californian data subjects, the applicable authority, and the required cope, as relevant.

Internal governance

-  Update your company's **internal Privacy and Data Protection Framework** in order to address the company's approach for its adherence to the CCPA.
-  Define your company **Data Protection Officer's** responsibility with respect to the CCPA, which should be reflected in an updated internal procedure.
-  **Train employees** as to the requirements under the CCPA, including the differences compared to the GDPR and on the handling of access requests.

HFN'S TECHNOLOGY & REGULATION DEPARTMENT

HFN's Technology and Regulation department is a recognized market leader in its field. The team is led by domain experts who possess vital regulatory skills in advising startups, multi-national companies, mobile apps and software developers, internet and disruptive technologies vendors, on the applicable technological regulatory and compliance considerations in numerous areas. These include privacy and data protection, cybersecurity, computer and software protection, content and advertising regulations, mobile and other app marketplaces compliance, specifically in the industries of adtech and online advertising, e-marketing, quality media and traffic; content, social networks and user generated content platforms; digital transformation; app monetization; health & lifestyle technologies; financial technology; and other e-commerce related operations.

The team has a thorough knowledge and diverse experience of the increasing volume of regulations, enforcement actions and legislative trends in a myriad of jurisdictions, including with respect to heavily "regulated" platforms, such as mobile marketplaces, browsers and other platforms, as well as industry best practices and leading self-regulatory guidelines. This enables the team members to offer unique and practical solutions for often complex situations and assist in the development, implementation and management of adequate procedures, in order to mitigate legal and business risks.

TEAM LEADERS

- [Dr. Nimrod Kozlovski](#)
Nimrod co-heads HFN's Technology & Regulation Department and is an expert investor in cybersecurity and a teaching professor on Internet and Cyber Law, information technology and innovation. Nimrod earned his doctoral degree in Law (J.S.D) from Yale Law School and conducted his post-doctoral research in Computer Science on Proactive Security at the Yale School of Computer Sciences.
- [Ariel Yosefi](#)
Ariel co-heads HFN's Technology & Regulation Department and is highly regarded for his global experience in advising multinational companies, developers, start-ups and others on regulatory and compliance matters surrounding data protection, cybersecurity and innovative technology compliance.
- [Ido Manor](#)
Ido is a partner in HFN's Technology & Regulation Department, specializing in advising Israeli and international clients, start-ups and internet companies, on a wide range of regulatory and commercial matters, involving data protection and privacy, online advertising, user-generated content, social media and mobile marketplaces compliance, e-commerce and international trade.
- [Israel \(Ruly\) Ber](#)
Ruly is a partner in HFN's Technology & Regulation Department. Ruly joined the department after 8 years as a legal advisor to one of Israel's largest banks. Ruly specializes in advising on data protection and privacy, online advertising, user-generated content, social media and mobile marketplace compliance, as well as financial and banking regulations, and their implications on financial institutions' information and technological procedures.
- [Dan Shalev](#)
Dan is a member of HFN's Technology & Regulation Department, specializing in advising on various technological and regulatory aspects, including online advertising and content, intellectual property, data protection and commercial matters. Dan began his legal career at prestigious Israeli law firms and has acquired unique, strategic, relevant experience for advising clients in the fields of online media, ad-tech, content and music production, having acted as VP and COO for two well-known, ad-tech companies and after co-founding the "Bama" Music School and a recording studio.