PAUL HASTINGS

COMPLIANCE CHECK – DO YOUR PRIVACY AND CYBERSECURITY PRACTICES COMPLY WITH THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA)?

PAUL HASTINGS

TABLE OF CONTENTS

OVERVIEW OF CCPA

The California Consumer Privacy Act (CCPA) became effective on ***January 1, 2020***, and aims to give California residents (referred to as "consumers") more control over the personal information ("PI") collected about them.

- **Personal Information**. PI is defined broadly under the CCPA as "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." PI does not include "information that is lawfully made available from federal, state, or local government records."
  - This definition encompasses typical "direct" identifiers (e.g., name, email address, physical address, social security number, passport number) but also online or other "indirect" identifiers, such as mobile advertising IDs, IP addresses, cookie IDs, user names, MAC addresses, or geolocation data.
- **Applicability**. The CCPA primarily applies to the following types of entities, to the extent they do business in California and *regardless of whether they are physically located in California or not*:
  - *Business*. A "business" is a for-profit entity that **(1)** collects consumers' PI (or direct the PI to be collected on their behalf), **(2)** determines the purposes and means of processing the consumers' PI, and **(3)** meets at least one of the following thresholds:
    - Has annual gross revenues in excess of $25 million;
    - Alone or in combination, annually buys, receives for a commercial purpose, sells, or shares for a commercial purpose, the PI of 50,000 or more consumers, households, or devices; or
    - Derives 50% or more of its annual revenues from selling PI.[1]
  - *Service Provider*. A "service provider" is a for-profit entity that processes consumers' PI on **behalf of a "business" pursuant to a written contract**.
    - In essence, this written contract will restrict the service provider to only using the PI to provide services on behalf of that business (with very limited exceptions for internal improvements to services).
- **Exemptions**. Until January 1, 2022, the CA legislature has largely carved out from the CCPA's requirements (with limited exception):
  - Employee (and job applicant) PI from the law's requirements until January 2022 - notably, however, businesses must still provide a short-form employee privacy notice; and
  - PI involved in "B2B" communications or transactions, where the communications or transactions solely relate to (a) providing or receiving a product or service to or from such entities or (b) due diligence of such entities.

[1] Please note that the CCPA also applies to any entity that "controls" or is "controlled" by a business subject to the CCPA and that shares "common branding" with such business.

- **Enforcement**. The California Attorney General began enforcing the CCPA on ***July 1, 2020***. The CCPA provides for civil penalties of up to $7,500 for each intentional violation of the law, and up to $2,500 for non-intentional violations. However, businesses have a 30-day period to "cure" (i.e., remediate) violations after being notified of alleged noncompliance.
- **Data Breach Litigation**. Under the CCPA, businesses have a duty to implement and maintain reasonable security procedures and practices to protect PI. The CCPA gives consumers the right to sue businesses (including via class actions) in the event that PI is accessed, exfiltrated, stolen, or disclosed without authorization as a result of the business's violation of this duty.
  - Consumers may recover statutory damages of $100-$750 per consumer per incident, or actual damages - whichever is greater, in addition to injunctive or declaratory relief, and "[a]ny other relief the court deems proper."
- **"Do Not Sell My Personal Information**." Essentially, the CCPA defines a "sale" of PI as any disclosure of PI to a third party for "monetary or other valuable consideration." Any business that "sells" PI must include a link entitled "Do Not Sell My Personal Information" on its website or mobile application (as applicable) to allow consumers to opt-out of such "sales."

The steps below can help you assess your company's compliance with the CCPA's requirements.

CCPA COMPLIANCE CHECKLIST

- **Create Awareness within Your Organization**. Whether you have already been operating in compliance with the CCPA for several months, or your business is just beginning to meet the CCPA's requirements, you should ensure that decision-makers and key individuals in your organization are aware of the CCPA and its impact on your business.
- **Understand the Information You Hold**. If you have not already done so, you should create data maps to document what PI you hold, how you use it, where you store it, the source of the PI, and with whom you share it. Among other things, this information is necessary for evaluating whether your company is a "business" or "service provider," engages in "sales" of PI, and can adequately respond to the consumer rights requests discussed below.
- **Communicate Your Data Use Practices**. Your privacy notices, both employee and consumer-facing, should be reviewed and updated to ensure compliance with specific CCPA disclosure requirements. You should also ensure that your company is collecting and processing PI in a manner consistent with these notices.
- **Recognize the Consumer Rights Granted by the CCPA**. Similar to the EU General Data Protection Regulation ("GDPR"), the CCPA creates a set of rights that consumers can request, specifically:
  - Right to know about PI collected, disclosed, or sold, including by receiving their "specific pieces" of PI (also known as "access requests");
  - Right to request deletion of PI;
  - Right to opt-out of the sale of PI; and
  - Right to non-discrimination for exercising these rights.
- **Create a Process for Responding to Access and Deletion Requests**. The rights listed above include the right of consumers to request copies of their specific PI and deletion of their PI, in either case, within forty-five (45) days. Your company should have a process for identifying this PI, verifying the consumer's identity (for fraud prevention purposes), and providing the copies in a clear, readable, and portable format. Your company should also have procedures in place for identifying what PI data must be deleted in response to a request, and what data may be retained according to any exceptions provided in the CCPA. Evaluating your response timeliness and completeness, on an ongoing basis, is critical to ensuring your continued compliance with CCPA.
- **Review All Transfers of PI to Third Parties**. Identify all transfers of PI to third parties and review whether they are transfers to a "service provider" or meet the definition of "sale" of data to a third party. You should execute contracts with third parties that are "service providers" making it clear that they may not use data under your agreement except as directed by your company.
- **Effective Mechanisms to Opt-Out of the Sale of PI**. Companies that "sell" PI must implement a process for consumers to opt-out of the sale of their PI, including by placing a "Do Not Sell My Personal Information" link on your website's homepage or mobile application's settings (as applicable). Where a company does not sell PI, this should be stated in the privacy notice to consumers.

- **Review Your Consent Mechanisms for Minors**. Companies that "sell" PI must also obtain the prior opt-in consent of consumers (or their guardians) under the age of 16.
- **Assess the Adequacy of Your Information Security Program**. The CCPA requires businesses to implement and maintain reasonable security procedures and practices to protect PI, especially due to the private right of action for data breaches. You should ensure your information security program is aligned with, and assessed against, the requirements of an established information security framework (e.g., CIS, NIST, or ISO).

HOW THE PAUL HASTINGS PRIVACY & CYBERSECURITY SOLUTIONS GROUP CAN HELP WITH CCPA COMPLIANCE

Our Privacy and Cybersecurity Solutions Group operates under our Global Privacy and Cybersecurity Practice Group and offers a unique blend of legal expertise and consultants under the umbrella of the law firm. This provides two important benefits to the CCPA compliance services that we provide to clients: 1) Our work can be delivered under attorney-client privilege and 2) Our recommendations have the weight and support of a respected, established, global law firm where we have reach-back capabilities to attorneys with deep experience in U.S. and international legal issues in the areas of privacy and cybersecurity. Furthermore, as a leading U.S. law firm, we have provided advice and support to hundreds of companies across all market sectors.

We can provide CCPA compliance support in any of the areas as listed above, and more specifically:

- **Document Review and Development**. We can enhance your current internal policies and procedures, as well as create new documentation to support your CCPA compliance program. Our team has extensive experience in creating program documentation that is both legally sufficient to meet regulatory requirements and customized to your unique business needs and functionality. We routinely work with clients to integrate CCPA compliance efforts into the broader compliance activities of the company, and while we have a library of tried-and-true templates, we work closely with our clients to ensure that any documents we produce are usable, workable guidelines that their businesses can easily follow.
- **Compliance Gap Assessment**. Based on the information provided above and our day-to-day experience in supporting CCPA compliance efforts at a broad range of companies, we can provide you with an easy-to-understand, actionable assessment that provides you a clear picture of where your program is now compared to where you need to be to comply with CCPA and in comparison to other similarly situated companies.
- **Remediation Roadmap Development**. Based on the compliance gap assessment, we can provide you with a prioritized, systematic guide for remediating those identified gaps, and provide guidance on who in your organization should be responsible for implementing each action item and what additional tools or resources you may need.
- **Data Mapping**. Our consultants are experienced at creating detailed data maps based on your documents and data collection, storage, sharing, and destruction practices. When necessary, we also collaborate with experienced technical firms to provide support for implementation and operationalization of data mapping tools.

OUR TEAM

Jacqueline Cooney

Leader, Privacy and Cybersecurity Group
Washington, DC
+1.202.551.1236
jacquelinecooney@paulhastings.com

John Binkley

Senior Director, Privacy and Cybersecurity Group
Washington, DC
+1.202.551.1862
johnbinkley@paulhastings.com

Daniel Julian

Director, Privacy and Cybersecurity Group
Washington, DC
+1.202.551.1231
danieljulian@paulhastings.com

Brianne Powers

Director, Privacy and Cybersecurity Group
Washington, DC
+1.202.551.1237
briannepowers@paulhastings.com

PAUL HASTINGS

ABOUT PAUL HASTINGS

Paul Hastings provides innovative legal solutions to many of the world's top financial institutions and Fortune 500 companies in markets across Asia, Europe, Latin America, and the United States.

We offer a complete portfolio of services to support our clients' complex, often mission-critical needs—from structuring first-of-their-kind transactions to resolving complicated disputes to providing the savvy legal counsel that keeps business moving forward.

Since the firm's founding in 1951, Paul Hastings has grown steadily and strategically along with our clients and the markets we serve. We established successful practices in key U.S. and European cities, creating a broad network of professionals to support our clients' ambitions. In addition, we were one of the first U.S. law firms to establish a presence in Asia, and today we continue to be a leader in the region. Over the past decade, we have significantly expanded our global network of lawyers to assist our clients in financial centers around the world, including the emerging markets of Latin America.

Today, we serve our clients' local and international business needs from offices in Atlanta, Beijing, Brussels, Century City, Chicago, Frankfurt, Hong Kong, Houston, London, Los Angeles, New York, Orange County, Palo Alto, Paris, San Diego, San Francisco, São Paulo, Seoul, Shanghai, Tokyo, and Washington, D.C.

Drawing on the firm's dynamic, collaborative, and entrepreneurial culture, our lawyers work across practices, offices, and borders to provide innovative, seamless legal counsel—where and when our clients need us.

Ranked among the Top 5 on the A-List of the most successful law firms in the U.S. six years in a row

— The American Lawyer

A top-ranked firm across Asia, Europe, and North America

— Financial Times' Innovative Lawyers Report

Named among the Top 5 Overall Best Law Firms to Work For four years in a row

— Vault's Annual Survey

Connect with us to keep current on the latest legal developments.

PAUL HASTINGS

GLOBAL RESOURCES

21 OFFICES *ACROSS THE AMERICAS, ASIA, AND EUROPE*

1 LEGAL TEAM *TO INTEGRATE WITH THE STRATEGIC GOALS OF YOUR BUSINESS*

THE AMERICAS

Atlanta
Century City
Chicago
Houston
Los Angeles
New York
Orange County
Palo Alto
San Diego
San Francisco
São Paulo
Washington, D.C.

ASIA

Beijing
Hong Kong
Seoul
Shanghai
Tokyo

EUROPE

Brussels
Frankfurt
London
Paris

PAUL HASTINGS

THE AMERICAS

Atlanta
1170 Peachtree Street, N.E.
Suite 100
Atlanta, GA 30309
t: +1.404.815.2400
f: +1.404.815.2424

Century City
1999 Avenue of the Stars
Los Angeles, CA 90067
t: +1.310.620.5700
f: 1.310.620.5899

Chicago
71 S. Wacker Drive
Forty-Fifth Floor
Chicago, IL 60606
t: +1.312.499.6000
f: +1.312.499.6100

Houston
600 Travis Street
Fifty-Eighth Floor
Houston, TX 77002
t: +1.713.860.7300
f: +1.713.353.3100

Los Angeles
515 South Flower Street
Twenty-Fifth Floor
Los Angeles, CA 90071
t: +1.213.683.6000
f: +1.213.627.0705

New York
200 Park Avenue
New York, NY 10166
t: +1.212.318.6000
f: +1.212.319.4090

Orange County
695 Town Center Drive
Seventeenth Floor
Costa Mesa, CA 92626
t: +1.714.668.6200
f: +1.714.979.1921

Palo Alto
1117 S. California Avenue
Palo Alto, CA 94304
t: +1.650.320.1800
f: +1.650.320.1900

San Diego
4747 Executive Drive
Twelfth Floor
San Diego, CA 92121
t: +1.858.458.3000
f: +1.858.458.3005

San Francisco
101 California Street
Forty-Eighth Floor
San Francisco, CA 94111
t: +1.415.856.7000
f: +1.415.856.7100

São Paulo
Av. Presidente Juscelino
Kubitschek, 2041
Torre D, 21º andar
São Paulo, SP, 04543-011
Brazil
t: +55.11.4765.3000
f: +55.11.4765.3050

Washington, DC
2050 M Street, N.W.
Washington, DC 20036
t: +1.202.551.1700
f: +1.202.551.1705

ASIA

Beijing
Suite 2601, 26/F
Yintai Center, Office Tower
2 Jianguomenwai Avenue
Chaoyang District
Beijing 100022, PRC
t: +86.10.8567.5300
f: +86.10.8567.5400

Hong Kong
21-22/F Bank of China Tower
1 Garden Road
Central Hong Kong
t: +852.2867.1288
f: +852.2523.2119

Seoul
33/F West Tower
Mirae Asset Center1
26, Eulji-ro 5-gil, Jung-gu,
Seoul 04539, Korea
t: +82.2.6321.3800
f: +82.2.6321.3900

Shanghai
43/F Jing An Kerry Center
Tower II
1539 Nanjing West Road
Shanghai 200040, PRC
t: +86.21.6103.2900
f: +86.21.6103.2990

Tokyo
Ark Hills Sengokuyama Mori
Tower
Fortieth Floor
1-9-10 Roppongi
Minato-ku Tokyo 106-0032
Japan
t: +81.3.6229.6100
f: +81.3.6229.7100

EUROPE

Brussels
Avenue Louise 480
1050 Brussels
Belgium
t: +32.2.641.7460
f: +32.2.641.7461

Frankfurt
TaunusTurm – Taunustor 1
60310 Frankfurt am Main
Germany
t: +49.69.907485.000
f: +49.69.907485.499

London
100 Bishopsgate
London EC2N 4AG
United Kingdom
t: +44.20.3023.5100
f: +44.20.3023.5109

Paris
32, rue de Monceau
75008 Paris
France
t: +33.1.42.99.04.50
f: +33.1.45.63.91.49