

# CCPA and GDPR: Comparison of certain provisions



**Steven R. Chabinsky**  
Global Data, Privacy & Cybersecurity  
**T** +1 202 626 3587  
**E** steven.chabinsky@whitecase.com



**F. Paul Pittman**  
Global Data, Privacy & Cybersecurity  
**T** +1 202 729 2395  
**E** paul.pittman@whitecase.com

Issue	CCPA	GDPR	Comments
<p><b>Scope: Covered Information &amp; Individuals</b></p>	<p>“Personal information” means information that: identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.</p> <p>This includes, without limitation:</p> <ul style="list-style-type: none"> <li>□ Identifiers such as a real name, alias, signature, physical characteristics or description, telephone number, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, passport number, driver’s license or state identification card number or other similar identifiers, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.</li> <li>□ Characteristics of protected classifications under California or federal law (for example, race, color, sex, age, religion, national origin, disability, citizenship status, and genetic information).</li> <li>□ Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.</li> <li>□ Biometric information.</li> </ul>	<p>“Personal data” meaning information relating to an identified or identifiable natural person (‘data subject’).</p> <p>An “identifiable natural person” is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[4]</p>	<p>Both laws focus on information that relates to a natural person who can be identified, albeit taking different approaches to the relevant definitions.</p> <p>As well as information that can be linked to a particular consumer (i.e., an individual), the CCPA also allows for information that can be linked with a particular <i>household</i>. In theory, this might make its scope broader than the GDPR. However, in practice, data that identifies a household (e.g., a home address for a family) is also likely to be “personal data” for the purposes of the GDPR.</p> <p>The CCPA explicitly identifies the relevant individuals (to which the personal information relates) as being California residents, whereas the GDPR does not limit the categories of individual (to which the personal data relates), <i>directly</i>. However, see “Covered Entities” row below.</p> <p>Organizations that are subject to both laws may see certain nuanced differences between the data about California residents that qualifies as “personal information” for the purposes of the CCPA and data that is “personal data” for the purposes of the GDPR. Consequently they may, for the purposes of compliance, either closely scrutinize such differences or take a “highest common denominator” approach.</p>

# CCPA and GDPR: Comparison of certain provisions

Issue	CCPA	GDPR	Comments
<p><b>Scope: Covered Information &amp; Individuals</b></p> <p><i>Continued</i></p>	<ul style="list-style-type: none"> <li>□ Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an Internet Website, application, or advertisement.</li> <li>□ Geolocation data.</li> <li>□ Audio, electronic, visual, thermal, olfactory, or similar information.</li> <li>□ Professional or employment-related information.</li> <li>□ Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act[1].</li> <li>□ Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.</li> </ul> <p>This excludes “publicly available” information, meaning information that is lawfully made available from federal, state or local government records unless that information is <i>used for a purpose that is not compatible with the purposes for which it is maintained and made available</i> in the government records for which it is publicly maintained.[2]</p> <p>“Consumer” means a natural person who is a California resident....however identified, including by any unique identifier.[3]</p>		

# CCPA and GDPR:

## Comparison of certain provisions

Issue	CCPA	GDPR	Comments
<p><b>Scope: Covered Entities</b></p>	<p>A “business,” means a for-profit legal entity (or sole proprietorship) collecting personal information about consumers that:</p> <ul style="list-style-type: none"> <li>□ either alone or jointly with others, determines the purpose and means of the processing of consumers’ personal information; <i>and</i></li> <li>□ does business in the State of California[5]; and <i>either</i></li> </ul> <p>A. has annual gross revenue over \$25,000,000;</p> <p>B. buys, sells, receives or shares for commercial purposes, the personal information of 50,000 or more consumers, devices or households, on an annual basis; <i>or</i></p> <p>C. derives 50 percent or more of their annual revenue from selling consumers’ personal information.[6]</p> <p>“Processing” means any operation or set of operations that are performed on personal data [sic] or on sets of personal data, whether or not by automated means[7].</p>	<p>Anyone who, as a controller <i>or processor</i>:</p> <ol style="list-style-type: none"> <li>1. processes personal data in the context of an EU establishment (whether or not the processing takes place in the EU); or</li> <li>2. without having an EU establishment, processes personal data of data subjects in the EU in relation to offering them goods or services, or monitoring their behavior.</li> </ol> <p>“Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data...[8]</p> <p>“Processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.[9]</p> <p>“Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means...[10]</p>	<p>The CCPA is narrower than the GDPR in a number of respects here; it applies only to entities that:</p> <ul style="list-style-type: none"> <li>□ are what would be referred to under the GDPR as “controllers”, and in fact the CCPA closely follows the language used in the GDPR’s definition of “controller” and “processing.”</li> <li>□ do business in California (unless every aspect of the entity’s commercial conduct takes place wholly outside of California), whereas the GDPR applies both: to processing taking place outside the EU (where the entity processes personal data in the context of an EU establishment) and to businesses with no EU establishment that are processing personal data about data subjects in the EU.</li> <li>□ exceed one of the applicable thresholds, whereas the GDPR has no such thresholds.</li> </ul>

# CCPA and GDPR: Comparison of certain provisions

Issue	CCPA	GDPR	Comments
<p><b>Disclosure / Transparency Obligations</b></p>	<p>At or before the point of collection, a business should inform consumers as to:</p> <ul style="list-style-type: none"> <li>□ the categories of personal information to be collected and</li> <li>□ the purposes for which the categories of personal information shall be used. [11]</li> </ul> <p>A business should disclose in its privacy policy (and update at least every 12 months):</p> <ul style="list-style-type: none"> <li>□ a description of consumers' specific rights under the CCPA[12] and the methods provided by the business for consumers to submit corresponding requests (including if the business sells personal information, a link to a "Do Not Sell My Personal Information" webpage).</li> <li>□ lists, in respect of the preceding 12 months, of:</li> <li>□ the categories of personal information collected, the sources from which such personal information is collected, the categories of third parties with whom such personal information is shared;</li> <li>□ the business or commercial purpose for collecting or selling personal information; and</li> <li>□ the categories of personal information disclosed (for a business purpose) or sold (or a statement that the business has not engaged in such sale or disclosure, if applicable).[13]</li> </ul>	<p>The controller is under an obligation to provide at the time of collection (when collecting from the data subject)[14]:</p> <ul style="list-style-type: none"> <li>□ the identity and the contact details of the controller;</li> <li>□ any recipients or categories of recipients of the personal data;</li> <li>□ the legal basis and purposes for the processing (if the controller then intends to process the personal data for a different purpose, it must inform the data subject before doing so);</li> <li>□ the retention period for the personal data, or if not possible, the criteria used to determine that period;</li> <li>□ the rights of access, rectification, deletion and portability of personal data, to restrict or object to processing and to complain to a supervisory authority;</li> <li>□ where applicable, information about: the controller's representative and data protection officer; the legitimate interests for processing; exports of the personal data out of the EEA; the right to withdraw consent</li> <li>□ whether the provision of personal data is required by law or in connection with a contract (and if the data subject is obligated to provide the personal data and the possible consequences of not doing so);</li> <li>□ any automated decision-making, including profiling, with at least meaningful information about the logic involved, the significance and the envisaged consequences for the data subject;</li> <li>□ the source of the personal data (where not obtained from the data subject).[15]</li> </ul>	<p>The scope of disclosures required by the GDPR extends beyond that required by the CCPA.</p> <p>Most of the types of information required to be disclosed by the CCPA are also required to be disclosed under the GDPR.</p> <p>However, even where the disclosure requirements are similar, there are some subtle differences. For example:</p> <ul style="list-style-type: none"> <li>□ while the GDPR undoubtedly requires disclosure if personal data is being sold, it does not include very prescriptive obligations of the kind reflected by the CCPA;</li> <li>□ the CCPA requires some disclosures only in respect of the previous 12 months, whereas the GDPR has no such limitation; and</li> <li>□ while both the GDPR and the CCPA require the disclosure of the rights available to applicable individuals, the rights themselves are also not identical.</li> </ul> <p>Therefore, existing privacy policies (even those tailored for the GDPR) will not automatically be fit-for-purpose for the CCPA and will likely need to be updated to reflect its requirements.</p>

# CCPA and GDPR: Comparison of certain provisions

Issue	CCPA	GDPR	Comments
<p><b>Right of Access (and portability)</b></p>	<p>A consumer has the right to disclosure from a business of the:</p> <p>A. information collected;</p> <p>B. categories of information collected;</p> <p>C. categories of third parties with whom the information is shared;</p> <p>D. categories of sources of the information;</p> <p>E. business or commercial purpose for collecting or selling personal information.</p> <p>A business that receives a verifiable request relating to the above is obligated (no more than twice in a 12-month period per consumer) to make the disclosure free of charge, within 45 days. The disclosure should be made in writing and delivered either: through the consumer’s account with the covered entity, if they have one (if not they should not be asked to create one); by mail; or electronically, at the consumer’s option if they do not have an account (in which case the information must be provided in a readily useable format that allows the consumer to easily transmit the information to another entity).[16]</p>	<p>A data subject has the right to confirmation from the controller about whether personal data about them is being processed; and, if so:</p> <ol style="list-style-type: none"> <li>I. a copy of the personal data;</li> <li>II. the categories of personal data concerned;</li> <li>III. the recipients or categories of recipient with whom the data may be shared (particularly outside the EEA or international organizations, with information about the corresponding safeguards);</li> <li>IV. any available information about the source (where not collected from the data subject);</li> <li>V. purposes of processing;</li> <li>VI. the existence of the rights of access, rectification, deletion and portability of personal data, to restrict or object to processing and to complain to a supervisory authority;</li> <li>VII. the retention period for the personal data, or if not possible, the criteria used to determine that period;</li> <li>VIII. any automated decision-making, including profiling, with at least meaningful information about the logic involved, the significance and the envisaged consequences for the data subject.[17]</li> </ol> <p>The controller generally is obligated to comply with a request free of charge[18] without undue delay and in any event within one month of receipt.[19] Where the request was made by electronic means,[20] and unless otherwise requested by the data subject, the information should be provided in a commonly used electronic form.</p> <p>In certain circumstances[21], a data subject has additional rights to:</p> <ul style="list-style-type: none"> <li>□ receive a copy of their personal data in a structured, commonly used, machine-readable format; and</li> <li>□ transmit the data to another controller without hindrance from the original controller, including to have the personal data transmitted directly from the first controller to the second controller.[22]</li> </ul>	<p>In both cases, the access right gives applicable individuals rights to obtain much of the same information that the business is also required to disclose in any event.</p> <p>The right of access are somewhat similar in some respects between the CCPA and the GDPR. In addition:</p> <ul style="list-style-type: none"> <li>□ the GDPR also gives data subjects the right to information about their other rights, although the CCPA does require the information about similar rights to be disclosed to consumers; and</li> <li>□ the GDPR is broader in scope than the CCPA, giving rights to information about the retention period and any automated decision-making.</li> </ul> <p>Beyond the right of access, the GDPR offers an additional “right to data portability” in certain circumstances. This allows a data subject to receive, and transmit/have transmitted to another controller, their personal data in a commonly used, machine-readable format. The CCPA goes part way towards a similar right, by providing that the a business responding to a consumer’s access request must (at the consumer’s option) provide the information electronically in a readily useable format that allows the consumer to easily transmit the information to another entity. However, unlike the GDPR, the CCPA does not go as far as to give a consumer a right to require the business itself to transfer the information to another business.</p> <p>Businesses that have implemented processes for responding to data subjects’ requests for access and portability under the GDPR may, in theory, be able to apply those processes in relation to the CCPA. However, not updating and tailoring those processes to the CCPA might miss nuanced differences in the relevant requirements and, in any event would involve the business “over-complying,” in particular by giving consumers a much wider scope of information than is required by the CCPA and by offering consumers rights (to portability to another business) that are not available under/required by the CCPA.</p>

# CCPA and GDPR: Comparison of certain provisions

Issue	CCPA	GDPR	Comments
<p><b>Right to Deletion / Erasure (“right to be forgotten”)</b></p>	<p>A consumer has the right to request deletion of personal information a business has collected from them.[23]</p> <p>A business that receives a verifiable request relating to the above is obligated to delete the consumer’s personal information from its records and direct any service providers to delete the consumer’s personal information from their records.[24]</p> <p>“Service provider” means a for-profit legal entity that processes information on behalf of a business and to which the business discloses a consumer’s personal information for a business purpose pursuant to a written contract (containing certain prohibitions).[25]</p> <p>Neither a business nor a service provider is required to comply with a consumer’s deletion request if the personal information is necessary for the business or service provider to:</p> <p>A. complete a transaction for which the personal information was collected, provide a good or service requested by the consumer or otherwise perform a contract between the business and the consumer;</p> <p>B. detect security incidents;</p> <p>C. protect against malicious, deceptive, fraudulent or illegal activity (or prosecute those responsible);</p> <p>D. debug to identify and repair functionality errors;</p> <p>E. exercise or ensure the right of another to exercise free speech or another legal right;</p> <p>F. comply with the California Electronic Communications Privacy Act, which compels the production of or access to electronic communication information or electronic device information with a search warrant;</p> <p>G. engage in research in the public interest (if the consumer has provided informed consent);</p> <p>H. to enable solely internal uses aligned with the consumer’s expectations given their relationship with the business;</p> <p>I. comply with a legal obligation;</p> <p>J. otherwise use the information internally in a lawful manner compatible with the context in which the consumer provided it.[26]</p>	<p>A data subject has the right to erasure by the controller of personal data about them in certain circumstances, namely if:</p> <ol style="list-style-type: none"> <li>I. the data is no longer needed for its original purpose (and no new lawful purpose exists);</li> <li>II. the processing is based on consent, and the data subject withdraws consent (and no other lawful ground exists);</li> <li>III. the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing;</li> <li>IV. the data has been processed unlawfully; or</li> <li>V. erasure is necessary to comply with EU or EU Member State law.[27]</li> </ol> <p>The controller is obligated to delete the data without undue delay and in any event within one month of receipt of the request.[28] The controller is also obligated notify to each recipient to whom the personal data has been disclosed (unless this proves impossible or involves disproportionate effort).[29]</p> <p>Where the controller has made the personal data public, the controller is obligated to take reasonable steps to inform other controllers processing the personal data that the data subject has requested deletion of any links to, or copy or replication of, that personal data.</p> <p>The deletion obligations do not apply where the processing:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> is necessary for exercising the right of freedom of expression and information;</li> <li><input type="checkbox"/> for compliance with EU or EU Member State law;</li> <li><input type="checkbox"/> for a task in the public interest or in the exercise of an official authority of the controller;</li> <li><input type="checkbox"/> in the public interest in public health;</li> <li><input type="checkbox"/> for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes,</li> <li><input type="checkbox"/> for the establishment, exercise or defense of legal claims.[30]</li> </ul>	<p>There are several differences between the deletion right (and corresponding obligations on businesses) under the CCPA and the GDPR:</p> <p>The CCPA’s deletion right applies only to data collected from the consumer (i.e. not to data about the consumer collected from third party sources), whereas the GDPR’s applies to all data concerning a data subject.</p> <p>While the CCPA and the GDPR have exceptions, in relation to which the applicable deletion right does not apply (see below), the GDPR also limits the circumstances in which the underlying right to deletion applies. However, these circumstances are broad enough to apply to most exercises of the right by data subjects.</p> <p>The exceptions to the CCPA’s deletion right are much broader than exceptions under the GDPR, and include circumstances such as where the information is needed: for a contract, free speech and internal uses aligned with the consumer’s expectations / the context in which the consumer provided the information. These are broad enough to potentially eliminate a consumer’s deletion rights under the CCPA in most, if not all, circumstances.</p> <p>A business that has implemented measures pursuant to the GDPR’s right to deletion (both to minimize and comply with requests) is unlikely to be able, or want, to simply apply the same measures to requests under the CCPA, and doing so would grant much broader deletion rights to consumers than are provided for by the CCPA. Instead, a close examination of the uses of personal information by the business and the corresponding circumstances in which the business will be obligated to comply with deletion requests should help the business both minimize and comply with requests under the CCPA.</p>

# CCPA and GDPR: Comparison of certain provisions

Issue	CCPA	GDPR	Comments
<b>Right to Opt-Out</b>	<p>A consumer has the right to require a business, that sells personal information to third parties, not to sell the consumer’s personal information (opt out).[31]</p> <p>A business is prohibited from selling personal information of a consumer:</p> <ul style="list-style-type: none"> <li>□ from whom it receives a request to opt out (unless and until it has subsequently received the consumer’s express authorization to do so.[32] which it cannot request for at least 12 months after receiving the opt-out request[33]).</li> <li>□ who is a minor if it has not received consent (i.e., opt in):</li> <li>□ whom the business has actual knowledge is under the age of 16, unless:               <ul style="list-style-type: none"> <li>□ the consumer is between 13 and 16 and has opted in; or</li> <li>□ the consumer is less than 13 years of age and the consumer’s parent or guardian has opted in on the consumer’s behalf.</li> </ul> </li> </ul> <p>“Sell”, “selling”, “sale”, or “sold” means selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating orally, in writing, or by electronic means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration.[34]</p>	<p>The GDPR does not include an express right for a data subject to opt out of the sale of their personal data.</p> <p>However, any controller processing personal data (including a business engaged in the sale of personal data) is subject to obligations under the GDPR not only to have (and inform data subjects about) a lawful basis for processing, but also, for example, to inform data subjects about the purposes of the processing and inform data subjects of their rights, in particular their rights to withdraw consent (if consent is the lawful basis) and/or object to such processing[35].</p>	<p>While the CCPA includes a specific right to opt out of the sale of personal information which the GDPR does not, the GDPR includes much broader rights for data subjects to restrict and object to the processing of their personal data more generally.</p> <p>Therefore, despite the absence of an express right to opt out (of data sale), the GDPR nevertheless presents significant challenges to any business that sells personal data (particularly as its business model).</p> <p>A business that sells personal data and has implemented measures pursuant to the GDPR is unlikely to find that those measures align with the requirements of the CCPA and is likely to need to implement separate measures in light of the CCPA (or to choose the “highest common denominator” approach).</p>

# CCPA and GDPR: Comparison of certain provisions

Issue	CCPA	GDPR	Comments
<b>Processors</b>	<p>The CCPA extends the right to deletion to include an obligation on a business to direct any service providers (entities to which the business has disclosed personal information for processing on behalf of the business) to comply with the deletion request (and, at least impliedly, the CCPA requires the service provider to comply with this request[36]).</p> <p>However, the CCPA does not otherwise include detailed obligations on or in relation to “processors” as such concept is understood in the GDPR.</p> <p>Service providers are liable for civil penalties under the CCPA just as businesses are, but are not liable for failure by a business that shares data with them to comply with its CCPA obligations.[37]</p>	<p>The GDPR includes detailed obligations both on: controllers in relation to processors; and on processors directly.</p>	<p>Businesses that engage processors that are “service providers” under the CCPA may want to seek to impose contractual obligations on such service providers to comply with deletion requests, e.g., in data processing agreements (that may have been implemented / updated pursuant to the GDPR.)</p> <p>Entities that act as service providers under the CCPA may consider both:</p> <ul style="list-style-type: none"> <li>□ anticipating notification from their CCPA business-customers of consumers’ deletion requests and implementing procedures to comply; and</li> <li>□ seeking to impose requirements on their CCPA business-customers to provide notification as required (e.g., in relevant data processing agreements, as above).</li> <li>□ Much like the GDPR, the CCPA may provoke detailed negotiations and “battles of the forms” as customers and vendors seek to impose contractual obligations on each other in relation to requirements of the CCPA—not only to comply with its requirements but also to control how the entity complies.</li> </ul>



# CCPA and GDPR: Comparison of certain provisions

- [1] 20 U.S.C. section 1232g, 34 C.F.R. Part 99
- [2] § 1798.140(o)
- [3] § 1798.140(g)
- [4] Art. 4(1)
- [5] The CCPA explicitly does not restrict a business's ability to collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California, which takes place if: the business collected that information while the consumer was outside of California, no part of the consumer's personal information occurred in California; and no personal information collected while the consumer was in California is sold.
- [6] § 1798.140(c)
- [7] § 1798.140(q)
- [8] Art. 4(7).
- [9] Art 4(8).
- [10] Art 4(2).
- [11] § 1798.100(b)
- [12] See further below.
- [13] §§ 1798.110(c); & 1798.130(a)(5)(B), (C).
- [14] When collecting from a third party: within a reasonable period after obtaining the data (but no more than one month); if used to communicate with the data subject, in the first communication; or if disclosing to another recipient, at latest when the data is first disclosed. There are certain limited exceptions to the obligation to provide information to the data subject when collection information about them from a third party.
- [15] Art. 13-14.
- [16] §§ 1798.100; 1798.110(a)-(b); 1798.130.
- [17] Art. 15.
- [18] Art. 12.5
- [19] Art. 12.3.
- [20] The controller should provide means for requests for all rights of data subjects under the GDPR to be made electronically, especially where personal data is processed by electronic means. Rec. (59).
- [21] Where the personal data processing is based on the data subject's consent or on a contract; and the processing is carried out by automated means. Art. 20.1.
- [22] Art. 20.
- [23] § 1798.105(a).
- [24] § 1798.105(c).
- [25] § 1798.140(v).
- [26] § 1798.105(d).
- [27] Art. 17.
- [28] Art. 12.3.
- [29] Art. 19.
- [30] Art. 17.
- [31] § 1798.120(a).
- [32] §§ 1798.120(c), 1798.135(a)(4).
- [33] § 1798.135(a)(5).
- [34] § 1798.140(t)(1), and § 1798.140(t)(2) includes detailed exceptions of when a business "does not sell personal information."
- [35] Art. 21.2. A data subject also has a specific right under Art. 21.3 to object to processing of their personal data for direct marketing purposes.
- [36] § 1798.105(d), which sets out a list of exceptions from the obligation to delete personal information in response to a consumer's request, provides that neither a business, nor "a service provider [is] required to comply with a consumer's request," at least suggesting by implication that, in all other circumstances (i.e., when none of the exceptions applies), the service provider is under an obligation to delete the personal information.
- [37] § 1798.145(h). For example, a service provider holding personal information provided by a business is not liable for that business's failure to comply with its obligations to delete that personal information upon request by a consumer.

## whitecase.com

In this publication, White & Case means the international legal practice comprising White & Case LLP, a New York State registered limited liability partnership, White & Case LLP, a limited liability partnership incorporated under English law, and all other affiliated partnerships, companies and entities. This publication is prepared for the general information of our clients and other interested persons. It is not, and does not attempt to be, comprehensive in nature. Due to the general nature of its content, it should not be regarded as legal advice.

Attorney Advertising. Prior results do not guarantee a similar outcome.