

# Privacy Law Comparison



GDPR



LGPD



PIPL



CCPA



CDPA



CPA






CTDPA








UCPA






	 <b>EU General Data Protection Act</b> GDPR	 <b>Brazil Lei Geral de Proteção de Dados</b> LGPD	 <b>China Personal Information Protection Law</b> PIPL
<b>Effective Date</b>	May 25, 2018	August 1, 2021	November 1, 2021
<b>Applicability</b>	<p><b>Data Controllers and Data Processors:</b></p> <ul style="list-style-type: none"> <li>Established in the EU that process personal data in the context of activities of the EU establishment, regardless of whether the data processing takes place within the EU.</li> <li>Not established in the EU that process EU data subjects' personal data in connection with offering goods or services in the EU, or monitoring their behavior.</li> </ul>	<p>The LGPD applies to any processing operation carried out, regardless of the location of the business, if any of the following apply:</p> <ul style="list-style-type: none"> <li>The processing is carried out within Brazil;</li> <li>The purpose of processing is to offer or provide goods or services to individuals located within Brazil; or</li> <li>The personal data processed is collected in Brazil.</li> </ul>	<p>Applies to the processing of personal information of natural persons within the territory of the People's Republic of China. It also applies to the processing of personal information of natural persons outside the People's Republic of China under any of the following circumstances:</p> <ul style="list-style-type: none"> <li>For the purpose of providing products or services to domestic natural persons;</li> <li>Analyze and evaluate the behavior of natural persons in the territory;</li> <li>Other circumstances stipulated by laws and administrative regulations.</li> </ul> <p><b>Personal information processors may process personal information only if one of the following circumstances is met:</b></p> <ul style="list-style-type: none"> <li>Obtain personal consent;</li> <li>Necessary for the conclusion and performance of a contract in which an individual is a party, or necessary for the implementation of human resource management in accordance with the labor rules and regulations established in accordance with the law and the collective contract signed in accordance with the law;</li> <li>It is necessary to perform statutory duties or statutory obligations;</li> <li>It is necessary to respond to public health emergencies, or to protect the life, health and property safety of natural persons in an emergency;</li> <li>Carry out news reports, public opinion supervision and other acts for the public interest, and handle personal information within a reasonable range;</li> <li>Processing personal information disclosed by individuals or other legally disclosed personal information within a reasonable scope in accordance with the provisions of this law;</li> <li>Other circumstances stipulated by laws and administrative regulations.</li> </ul>






\* indicates that this provision will come into effect January 1, 2023 under CPRA

	 <b>California Consumer Protection Act</b> CCPA	 <b>Virginia Consumer Data Protection Act</b> CDPA	 <b>Colorado Privacy Act</b> CPA	 <b>Connecticut Data Privacy Act</b> CTDPA	 <b>Utah Consumer Privacy Act</b> UCPA
<b>Effective Date</b>	January 1, 2020 * January 1, 2023	January 1, 2023	July 1, 2023	July 1, 2023	December 31, 2023
<b>Applicability</b>	<p>For-profit entities that collect personal information from California residents and meet any of the following thresholds:</p> <ul style="list-style-type: none"> <li>At least \$25 million in gross annual revenue</li> <li>Buys, sells or receives personal information about at least 50,000 California consumers, householders or devices for commercial purposes or</li> <li>Derives more than 50% of its annual revenue from the sale of personal information</li> </ul> <p>* (ii) above is replaced with "buys, sells or shares personal information of 100,000 or more California residents or households"</p> <p>(iii) above is replaced with "derives 50% or more of annual revenue from selling or sharing California personal information."</p>	<p>For-profit entities that conduct business in Virginia or offer products or services targeted to residents in Virginia and</p> <ul style="list-style-type: none"> <li>Control or process the data of at least 100,000 consumers or</li> <li>Control or process the data of at least 25,000 consumers and derive more than 50% of revenue from the sale of personal data</li> </ul>	<p>The law applies to legal entities that:</p> <ul style="list-style-type: none"> <li>Conduct business or produce products or services that are intentionally targeted to Colorado residents and</li> <li>Either control or process personal data of more than 100,000 consumers per calendar year or</li> <li>Derive revenue or receive a discount on the price of goods or services from the sale of personal data and control or process the personal data of at least 25,000 consumers.</li> </ul>	<p>Applies to persons that conduct business in Connecticut or that produce products or services that are targeted to Connecticut residents and that during the preceding calendar year:</p> <ul style="list-style-type: none"> <li>Controlled or processed the personal data of at least 100,000 consumers (excluding personal data controlled or processed to complete payment transactions); or</li> <li>Controlled or processed the personal data at least 25,000 consumers and derived more than 25% gross revenue from the sale of personal data.</li> </ul>	<p>Data Controllers and Data Processors who "conduct business in the state" or "[produce] a product or service that is targeted to consumers who are residents of the state."</p> <p><b>Covered entities must meet a small business threshold of over \$25 million in annual revenue and satisfy at least one of the following thresholds:</b></p> <ul style="list-style-type: none"> <li>During a calendar year, controls or processes personal data of 100,000 or more consumers or</li> <li>Derives over 50% of the entity's gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers.</li> </ul>




\* indicates that this provision will come into effect January 1, 2023 under CPRA

	 <b>GDPR</b>	 <b>LGPD</b>	 <b>PIPL</b>
<b>Covered Personal Information</b>	<p>Personal data is any information relating to an identified or identifiable data subject.</p> <p>The GDPR prohibits processing of defined special categories of personal data unless a lawful justification for processing applies.</p>	<p>“Personal data” means “information regarding an identified or identifiable natural person.”</p>	<p>Personal information is a variety of information related to an identified or identifiable natural person recorded electronically or by other means, excluding anonymized information.</p> <p>The processing of personal information includes the collection, storage, use, processing, transmission, provision, disclosure, deletion, etc. of personal information.</p>
<b>Sensitive Data</b>	<p>The following personal data is considered ‘sensitive’ and is subject to specific processing conditions:</p> <ul style="list-style-type: none"> <li>• Racial or ethnic origin</li> <li>• Political opinions</li> <li>• Religious or philosophical beliefs</li> <li>• Trade-union membership</li> <li>• Genetic data</li> <li>• Biometric data processed solely to identify a human being</li> <li>• Health-related data</li> <li>• Sex life or sexual orientation</li> </ul>	<p>“The processing of sensitive personal data is restricted to two situations per Article 11. First, when the data subject has given his/her specific consent for specific purposes. Second, in the absence of consent, when the processing is indispensable for certain specified purposes (e.g., compliance with a legal obligation, protecting life or physical safety, and fraud prevention).</p> <p>The law defines “sensitive personal data” as “personal data concerning racial or ethnic origin, religious belief, political opinion, trade union or religious, philosophical or political membership, data concerning health or sex life, genetic or biometric data, when related to a natural person.”</p>	<p>Sensitive personal information is personal information that, once leaked or used illegally, can easily lead to the infringement of the personal dignity of natural persons or the harm of personal and property safety, including biometrics, religious beliefs, specific identities, medical health, financial accounts, Information such as whereabouts, as well as personal information of minors under the age of fourteen.</p> <p>Personal information processors can process sensitive personal information only when they have a specific purpose and sufficient necessity, and take strict protective measures.</p> <p>The processing of sensitive personal information shall obtain the individual’s individual consent; where laws and administrative regulations provide that the processing of sensitive personal information shall obtain written consent, the provisions shall be followed.</p> <p>When processing sensitive personal information, personal information processors shall, in addition to the matters specified in the first paragraph of Article 17 of this law, also inform individuals of the necessity of processing sensitive personal information and the impact on personal rights and interests; in accordance with this law.</p> <p>The law stipulates that the individual may not be notified except.</p>

\* indicates that this provision will come into effect January 1, 2023 under CPRA

	 <b>CCPA</b>	 <b>CDPA</b>	 <b>CPA</b>	 <b>CTDPA</b>	 <b>UCA</b>
<b>Covered Personal Information</b>	<p>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.</p>	<p>Any information that is linked or reasonably associated to an identified or identifiable natural person – also includes households</p>	<p>CPA defines “personal data” as “information that is linked or reasonably linkable to an identified or identifiable individual,” with the exceptions of (a) de-identified data and (b) publicly available information.</p>	<p>“Personal data” means any information that is linked or reasonably linkable to an identified or identifiable individual. “Personal data” does not include de-identified data or publicly available information.</p>	<p>The Act covers the collection, processing, and sharing of personal data, defined as “information that is linked or reasonably linkable to an identified or identifiable individual.” The Act excludes “deidentified data,” “aggregated data,” and “publicly available information” from the scope of covered data. The Act also defines and establishes additional protections for “sensitive data” and certain carve-outs of “pseudonymous data”.</p>
<b>Sensitive Data</b>	<p>Not currently covered</p> <p>* New categories of “sensitive personal information,” including:</p> <ul style="list-style-type: none"> <li>• Social Security numbers (SSNs),</li> <li>• Driver’s license</li> <li>• Financial account or card numbers</li> <li>• Precise geolocation</li> <li>• Racial and ethnic characteristics</li> <li>• Religious and philosophical beliefs</li> <li>• Union membership,</li> <li>• Contents of mail, email and text messages</li> <li>• Genetic and biometric data</li> </ul>	<p>Consent is required to process “sensitive data” which includes racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship or immigration status, biometric data, personal data collected from a known child and precise geolocation data.</p>	<p>Sensitive data is defined as:</p> <ul style="list-style-type: none"> <li>• Personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status</li> <li>• Genetic or biometric data that may be processed for the purpose of uniquely identifying an individual, or</li> <li>• Data from a known child</li> </ul>	<p>Consent is required to process “sensitive data” which includes racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship or immigration status, biometric data, personal data collected from a known child and precise geolocation data.</p>	<p>Controllers are prohibited from processing sensitive data collected from a consumer without first presenting the consumer with clear notice and an opportunity to opt out.</p> <p>A controller “may not process sensitive data collected from a consumer without first presenting the consumer with clear notice and an opportunity to opt out of the processing”. This opt-out right for sensitive data also applies to all personal information, including pseudonymous data, although it is subject to the generalized exemptions in the law (for e.g., detecting fraud, defending legal claims, as well as not re-identifying pseudonymous or deidentified data, etc.).</p> <p><b>Sensitive data is defined as:</b></p> <ul style="list-style-type: none"> <li>• Personal data that reveals racial or ethnic origin, religious beliefs, sexual orientation, citizenship or immigration status, or “information regarding an individual’s medical history, mental or physical health condition, or medical treatment or diagnosis by a healthcare professional”</li> <li>• The processing of genetic or biometric data for the purpose of identifying a specific individual; and</li> </ul> <p>Specific geolocation data (§13-61-101(32)). Sensitive data does not include racial or ethnic origin if the data is processed by a “video communication service,” or a person licensed to provide healthcare.</p>

\* indicates that this provision will come into effect January 1, 2023 under CPRA

	 <b>GDPR</b>	 <b>LGPD</b>	 <b>PIPL</b>
<p><b>Anonymous, De-identified, Pseudonymous, or Aggregated Data</b></p>	<p>Pseudonymous data is considered personal data.</p> <p>Anonymous data is not considered personal data.</p> <p>While the GDPR does not mention de-identified data, the CCPA definition is similar to GDPR's concept of anonymous data.</p>	<p>Under LGPD, businesses must comply with LGPD regulation regardless of the data type.</p>	<p>Personal information is a variety of information related to an identified or identifiable natural person recorded electronically or by other means, excluding anonymized information.</p>
<p><b>Privacy Notice</b></p>	<p>Data Controllers must provide detailed information about its personal data collection and Data Processing activities. The notice must include specific information depending on whether the data is collected directly from the data subject or a third party.</p>	<p>Controllers are required to notify data subjects of the following:</p> <ul style="list-style-type: none"> <li>• The specific purposes of processing;</li> <li>• The type and duration of processing;</li> <li>• The controller's identity;</li> <li>• The controller's contact details;</li> <li>• Information regarding any sharing activities with other controllers and the purpose of sharing;</li> <li>• The responsibilities of the agents carrying out the processing; and</li> <li>• The data subject rights under the LGPD.</li> </ul> <p>The LGPD does not specify that this must be provided before the collection of personal data. Still, these notice disclosures likely should be included within your organization's privacy policy if within the scope of the LGPD.</p>	<p>Before processing personal information, personal information processors shall truthfully, accurately and completely inform individuals of the following matters in a conspicuous manner and in clear and easy-to-understand language:</p> <ul style="list-style-type: none"> <li>• The name or name and contact information of the personal information processor;</li> <li>• Purpose of processing personal information, processing method, type of personal information processed, and retention period;</li> <li>• Methods and procedures for individuals to exercise their rights under this law;</li> <li>• Other matters that should be notified by laws and administrative regulations.</li> </ul> <p>If there is a change in the matters specified in the preceding paragraph, the individual shall be notified of the changed part.</p> <p>Where the personal information processor informs the matters specified in the first paragraph by formulating personal information processing rules, the processing rules shall be made public, and shall be convenient for inspection and storage.</p>

\* indicates that this provision will come into effect January 1, 2023 under CPRA



CCPA



CDPA



CPA



CTDPA



UCA

**Anonymous, De-identified, Pseudonymous, or Aggregated Data**

The CCPA does not restrict a business's ability to collect, use, retain, sell, or disclose a consumer information that is deidentified or aggregated.

However, the CCPA establishes a high bar for claiming data is deidentified or Aggregated Pseudonymous data may qualify as personal information under the CCPA because it remains capable of being associated with a particular consumer or household. However, the statute does not clearly categorize or exclude pseudonymous data as personal information.

The definition of persona data goes on to explicitly exclude "de-identified data or publicly available information," but not pseudonymous information.

"De-identified data" means data that do not identify an individual with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.

"Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information, provided such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

"Deidentified data" is data that "cannot reasonably be linked to an identified or identifiable individual". Deidentified data must also be possessed by a controller who:

- Takes reasonable measures to ensure that a person cannot associate the data with an individual
- Publicly commits to maintain and use the data only in deidentified form and not attempt to reidentify the data, and
- Contractually obligates any recipients of the data to comply with these requirements.

\* indicates that this provision will come into effect January 1, 2023 under CPRA



CCPA



CDPA



CPA



CTDPA



UCA

**Privacy Notice**

Businesses must inform consumers about:

- The personal information categories collected.
- The intended use purposes for each category.

Further notice is required to:

- Collect additional personal information categories.
- Use collected personal information for unrelated purposes.

The CCPA requires that businesses provide specific information to consumers and establishes delivery requirements.

Third parties must also give consumers explicit notice and an opportunity to opt out before re-selling personal information that the third party acquired from another business.

“CDPA does not expressly require businesses to display a privacy notice at or before the point of the collection of personal data, nor does it require businesses to provide a “do not sell my information” link.

There is an obligation to post a privacy notice and specific requirements for what must be included, including all intended purposes for use of the personal data.”

Duty of transparency: The controller must provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

- The categories of personal data collected or processed by the controller or a processor;
- The purposes for which the categories of personal data are processed;
- An estimate of how long the controller may or will maintain the consumer’s personal data;
- An explanation of how and where consumers may exercise their rights under SB 21-190;
- The categories of personal data that the controller shares with third parties, if any; and
- The categories of third parties, if any, with whom the controller shares personal data.

Mandates that controllers provide consumers with a privacy notice with the following information:

- The categories of personal data processed;
- The purposes for which the categories of personal data are processed;
- How consumers may exercise a right;
- The categories of personal data that the controller shares with third parties;
- The categories of third parties with whom the controller shares personal data; and
- An active electronic mail address or other online mechanism that the consumer may use to contact the controller.

Incorporates privacy by design principles, including requiring controllers to:

- Limit the collection of data to what is adequate, relevant and reasonably necessary in relation to the purpose for which data is processed (as disclosed to customers),
- Not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which the data is being processed (unless the controller obtains consent), and
- Establish, implement, and maintain data security practices, among other requirements.

A controller is required to provide consumers with a “reasonably accessible and clear privacy notice” that includes:

- The categories of personal data processed by the controller
- The purposes for which the categories of personal data are processed
- How consumers may exercise a right
- The categories of personal data that the controller shares with third parties, if any; and
- The categories of third parties, if any, with whom the controller shares personal data

\* indicates that this provision will come into effect January 1, 2023 under CPRA





GDPR



LGPD



PIPL

**Consumer Rights**

**Rights include:**

- Information
- Access
- Rectification
- Erasure
- Restriction of Processing
- Data Portability
- Objection
- Avoid Automated Decision-Making

**Article 9 provides data subjects with the right to receive notice of:**

- The specific purposes of the processing,
- The type and duration of the processing,
- The controller's identity and contact information,
- Information regarding the shared use of the data by the controller and the purpose,
- Responsibilities of the agents that will carry out the processing, and
- An explanation of the data subjects rights.

**Article 18 allows data subjects to make a request to obtain:**

- Confirmation of existence of processing;
- Correction of incomplete, inaccurate or out-of-date data;
- Anonymization, blocking or deletion of unnecessary or excessive data or data processed in noncompliance with the provisions of LGPD;
- Data portability;
- Deletion of personal data processed with the data subject's consent (subject to certain exceptions); (6)
- Information about public and private entities with which the controller has shared data;
- Information about the possibility of denying consent and the consequences of such denial; (8) revocation of consent.

**Rights include:**

- Individuals have the right to know and make decisions about the processing of their personal information, and have the right to restrict or refuse the processing of their personal information by others; unless otherwise provided by laws and administrative regulations.
- Individuals have the right to consult and copy their personal information to the personal information processor; except under the circumstances specified in Article 18, paragraph 1, and Article 35 of this law.
- Where an individual requests to view or copy his personal information, the personal information processor shall provide it in a timely manner.
- Individuals requesting the transfer of personal information to their designated personal information processor, and the personal information processor shall provide the means for the transfer if the conditions specified by the national cybersecurity and informatization department are met.
- If an individual discovers that his or her personal information is inaccurate or incomplete, he has the right to request the personal information processor to correct or supplement it.
- Where an individual requests correction or supplement of his personal information, the personal information processor shall verify his personal information and make corrections and supplements in a timely manner.
- Individuals have the right to request personal information processors to explain their personal information processing rules.
- In the event of a natural person's death, his close relatives may, for their own lawful and legitimate interests, exercise the rights of access, copy, correction, deletion, etc., to the relevant personal information of the deceased as provided in this chapter; unless otherwise arranged by the deceased during his lifetime.

\* indicates that this provision will come into effect January 1, 2023 under CPRA



CCPA



CDPA



CPA



CTDPA



UCPA

**Consumer Rights**

**Rights include:**

- Know and access
- Deletion
- Opt out of sale (more broadly defined as the exchange of personal information for monetary or other valuable consideration)
- Nondiscrimination
- Data portability
- \* Rectification and correction
- \* Opt out of sharing for cross-context behavioral advertising
- \* Limit use and disclosure of sensitive personal information
- \* Opt out of the use of automated decision-making

**Rights include:**

- Know, access and confirm
- Deletion
- Opt out of sale (defined as the exchange of personal data for monetary consideration)
- Opt out of processing for targeted advertising
- Opt out of profiling
- Nondiscrimination
- Data portability
- Rectification/correction

**Rights include:**

- Right to opt out of the processing of personal data concerning the consumer;
- Right to access the consumer's personal data and confirm whether a controller is processing personal data concerning the consumer;
- Right to correct inaccurate personal data collected from the consumer;
- Right to delete personal data concerning the consumer;
- Right to obtain the consumer's personal data in a portable and readily usable format up to two times per calendar year

**Rights include:**

- The right to confirm whether a controller is processing their personal data, and the right to access their personal data;
- The right to correct inaccuracies in their personal data;
- The right to delete the personal data provided to the controller;
- The right to obtain a copy of their personal data in a format that is portable, readily usable, and allows the consumer to transmit the data to another controller without hindrance; and
- The right to opt out of the processing of their personal data for the purposes of
  - Targeting advertising,
  - The sale of personal data, or
  - Profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

**Rights include:**

- Confirm whether a controller is processing the consumer's personal data and access that personal data
- Delete (only to data that a consumer has provided to a controller, excluding derived and inferred data as well as data collected from third parties)
- Portability
- Opt out of targeted advertising , sensitive data, and sales including to pseudonymous data

**No Rights for:**

- Correction
- Profiling

**The Act also does not contain specific secondary use limitations that can be construed to apply to secondary uses of data for research.**

\* indicates that this provision will come into effect January 1, 2023 under CPRA



GDPR



LGPD



PIPL

**Contracting**

Requires controllers to enter into contracts with Processors to govern the processing of personal data by a processor on behalf of the controller.

The contract should include:

- Type of data
- Duration of processing
- The rights and obligations of both parties, with specific obligations for the processor

Unlike the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') in the EU, the LGPD does not expressly require organisations (both as controllers or processors) to execute contracts when there is shared use of personal data with third parties, including the vendors. Sector-specific laws, such as those of the financial sector, may require the execution of a contract with vendors.

When a personal information processor entrusts the processing of personal information, it shall agree with the trustee on the purpose, time limit, processing method, types of personal information, protection measures, and the rights and obligations of both parties, etc., and the trustee's Supervise personal information processing activities.

The trustee shall process personal information in accordance with the agreement, and shall not process personal information beyond the agreed processing purpose, processing method, etc.; if the entrustment contract is not effective, invalid, revoked or terminated, the trustee shall return the personal information to the personal information processor or delete it, Shall not be retained.

If a personal information processor really needs to provide personal information outside the People's Republic of China due to business needs, it shall meet one of the following conditions:

- Enter into a contract with the overseas recipient in accordance with the standard contract formulated by the national cyberspace administration department, stipulating the rights and obligations of both parties

\* indicates that this provision will come into effect January 1, 2023 under CPRA



CCPA



CDPA



CPA



CTDPA



UCPA

**Contracting**

Mandatory contracting requirements for “service providers” and “third parties” to whom the company does not sell data.

\* Mandatory contracting requirements for “contractors” to whom the company makes available personal information for a business purpose.

Requires controllers to enter into contracts with processors to govern the processing of personal data by a processor on behalf of the controller.

The contract should include:

- Type of data
- Duration of processing
- The rights and obligations of both parties, with specific obligations for the processor

Similar to preceding data privacy legislation, CPA utilizes concepts of data “controllers” and data “processors,” where a “controller” is the person or entity that determines the purposes and means of processing personal data and the “processor” is the person or entity that processes personal data on behalf of the controller.

Controllers and processors must enter into a binding contract governing the processing instructions. Controllers do not avoid responsibility by delegating processing responsibilities to a processor.

Requires controllers to enter into contracts with processors to govern the processing of personal data by a processor on behalf of the controller.

A processor is required to adhere to the instructions of the controller and assist the controller to meet its obligations under the Act “insofar as reasonably practicable,” including obligations under Utah’s breach notification law.

A contract between a controller and processor must be adopted that includes the following elements:

- Setting forth instructions for processing including the duration and each parties’ rights and obligations
- Requiring the processor to ensure each person processing personal data is subject to a duty of confidentiality
- Requires the processor to engage any subcontractor pursuant to a written contract that contains the same obligations.

\* indicates that this provision will come into effect January 1, 2023 under CPRA



GDPR



LGPD



PIPL

### Data Protection Assessments

GDPR Article 35, requires data protection assessments when processing personal data for certain functions such as targeted advertising, the sale of the data, certain types of profiling, the processing of sensitive data, and processing that presents a heightened risk of harm to consumers.

LGPD requires organizations to appoint a Data Protection Officer, conduct data privacy impact reports, maintain records of processing activities, comply with specific consent requirements, and implement security, technical, and administrative measures to protect personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, alteration, communication or any type of improper or unlawful processing.

Personal information processed by state agencies shall be stored within the territory of China; if it is indeed necessary to provide it overseas, a security assessment shall be conducted.

If a personal information processor needs to provide personal information outside the China due to business needs, it shall meet one of the following conditions:

- Pass the security assessment organized by the national cybersecurity and informatization department in accordance with the provisions of Article 40 of this Law;
- Conduct personal information protection certification by professional institutions in accordance with the regulations of the national cyberspace administration;
- Enter into a contract with the overseas recipient in accordance with the standard contract formulated by the national cyberspace administration department, stipulating the rights and obligations of both parties;
- Other conditions stipulated by laws, administrative regulations or national cyberspace administration departments.

Personal information processors shall regularly conduct compliance audits of their processing of personal information in compliance with laws and administrative regulations. In any of the following circumstances, the personal information processor shall conduct a personal information protection impact assessment in advance and record the processing situation

- Processing sensitive personal information;
- Using personal information to make automated decision-making;
- Entrust the processing of personal information, provide personal information to other personal information processors, and disclose personal information;
- Providing personal information abroad;
- Other personal information processing activities that have a significant impact on personal rights and interests.

Assessment of the impact of personal information protection shall include the following:

- Whether the processing purpose and processing method of personal information are legal, proper and necessary;
- Impact on personal rights and security risks;
- Whether the protective measures adopted are legal, effective and compatible with the degree of risk

\* indicates that this provision will come into effect January 1, 2023 under CPRA



CCPA



CDPA



CPA



CTDPA



UCPA

**Data Protection Assessments**

Not currently required

\* Under CPRA Cybersecurity audits and risk assessments will be required for companies whose processing presents a significant risk to consumer privacy or security

Yes, for the following processing activities:

- The processing of personal data for targeted advertising
- The sale of personal data
- The processing of personal data for purposes of profiling
- The processing of sensitive data

Processing activities involving personal data that present a heightened risk of harm to consumers.

Yes, before engaging in processing that presents a heightened risk of harm to a consumer, a controller must conduct and document a data protection assessment of each of its processing activities that involves personal data acquired on or after the effective date of CPA.

CPA defines “processing that presents a heightened risk of harm to a consumer” as including the following:

- Processing personal data for purposes of targeted advertising or profiling;
- Selling personal data; and
- Processing sensitive data.

Yes




Documented impact assessments are required when a controller’s processing activities present a heightened risk of harm to a consumer. These include.

- Processing personal data for purposes of targeted advertising;
- The sale of personal data;
- Processing personal data for purposes of profiling in cases of significant consumer risk or injury; and
- Processing sensitive data.






The UCPA lacks requirements to conduct either privacy or security risk assessment.

However, the UCPA’s data security program requirement does instruct controllers to reduce reasonably foreseeable risks of harm to consumers.

\* indicates that this provision will come into effect January 1, 2023 under CPRA




	 <b>GDPR</b>	 <b>LGPD</b>	 <b>PIPL</b>
<b>Enforcement</b>	Enforced by the European Data Protection Board as well as binding decision-making by the Data Protection Authorities of the member states.	Brazilian Data Protection Authority, the ANPD.	The State Cyberspace Administration is responsible for overall planning and coordination of personal information protection and related supervision and management. The relevant departments of the State Council shall be responsible for personal information protection and supervision and management within the scope of their respective duties in accordance with the provisions of this Law and relevant laws and administrative regulations.
<b>Private Right of Action</b>	None	Yes	None
<b>Penalties and Damages</b>		Violations of the LGPD may result in fines of up to 2% of the organization's global revenue for the prior year up to a total of 50 million reais (or approximately USD 9.3 million) per violation.	

\* indicates that this provision will come into effect January 1, 2023 under CPRA






	 <b>CCPA</b>	 <b>CDPA</b>	 <b>CPA</b>	 <b>CTDPA</b>	 <b>UCPA</b>
<b>Enforcement</b>	Enforced by the attorney general	Enforced by the attorney general	Colorado Attorney General and District Attorneys.	Enforced by the attorney general	Division of Consumer Protection Utah Department of Commerce Attorney General  The UCPA provides for the creation of a Consumer Privacy Restricted Account funded by civil fines assessed under the Act. The Consumer Privacy Restricted Account will be used to support investigation costs by the Division of Consumer Protection, recover costs and fees accrued by the Attorney General, and provide consumer and businesses education regarding consumer rights. Should the balance in the account exceed \$4,000,00 at the close of a fiscal year, any exceeding amount will be transferred into the General Fund.  The UCPA requires the Attorney General and the Division of Consumer Protection to submit a Report evaluating the effectiveness of enforcement efforts and summarizing information protected and not protected under the Act. This report is to be submitted to the Business and Labor Interim Committee before July 1, 2025.
<b>Private Right of Action</b>	Limited private right of action for breach of unredacted or unencrypted personal information due to failure to maintain reasonable security practices.	None	None	None	None
<b>Penalties and Damages</b>	Up to \$2,500 for each violation and \$7,500 for each intentional violation  * Automatic \$7,000 fine for a violation involving the personal information of minors  Statutory damages from \$100-\$750 per violation.	Up to \$7,500 for each violation	Violations would be subject to civil penalties under the CPA, which provides for civil penalties of not more than \$20,000 per violation.	None	None

\* indicates that this provision will come into effect January 1, 2023 under CPRA



	 <b>GDPR</b>	 <b>LGPD</b>	 <b>PIPL</b>
<b>Cure Period</b>	None	None	None
<b>Exemptions</b>	<p>The only way to be exempt from the GDPR is if you:</p> <ul style="list-style-type: none"> <li>Actively discourage the processing of data from EU data subjects (i.e., block your site in the EU) Process personal data of EU citizens outside the EU as long as you don't directly target EU data subjects or monitor their behavior</li> </ul>	<p>LGPD does exempt the processing of personal data by natural persons exclusively for private and non-economic purposes, journalistic and artistic purposes, academic purposes (subject to certain exemptions), or processing that is done exclusively for public safety, national defense, state security, or activities of investigation and prosecution of criminal offenses (which processing is subject to separate obligations).</p>	None
<b>Children</b>	<p>The GDPR's default age for consent is 16, although individual member state law may lower the age to no lower than 13. The person with parental responsibility must provide consent for children under the consent age.</p> <p>Children must receive an age appropriate privacy notice.</p> <p>Children's personal data is subject to heightened security requirements.</p>	<p>In general, Article 14 requires parental consent to process children and adolescents' personal data. The requirements of Article 14 are similar to those in the Children's Online Privacy Protection Act.</p>	<p>When a personal information processor handles the personal information of a minor under the age of fourteen, it shall obtain the consent of the minor's parent or other guardian.</p> <p>Personal information processors who process the personal information of minors under the age of fourteen shall formulate special personal information processing rules.</p>

\* indicates that this provision will come into effect January 1, 2023 under CPRA

	 <b>CCPA</b>	 <b>CDPA</b>	 <b>CPA</b>	 <b>CTDPA</b>	 <b>UCPA</b>
<b>Cure Period</b>	<p>Yes, 30 days for Attorney General enforcement</p> <p>* Removes the 30-day cure period and gives the Agency discretionary power to provide the business with a time period to cure</p>	None	Yes, the Act establishes a right to cure period of 60 days. This cure period will be repealed January 1, 2025	<p>Yes</p> <p>A sixty-day cure period once AG provides written notice of alleged violation, between the period of July 1, 2023 to December 31, 2024. Starting January 1, 2025, the bill provides the AG discretion to provide an opportunity to correct an alleged violation."</p>	30 Days
<b>Children</b>	<p>The CCPA prohibits selling personal information of a consumer under 16 without consent.</p> <p>Children aged 13-16 can directly provide consent.</p> <p>Children under 13 require parental consent.</p> <p>Protections provided in the Children's Online Privacy Protection Act (COPPA) still apply on top of the CCPA's requirements.</p>	Up to \$7,500 for each violation	<p>A controller must not process sensitive data concerning a consumer without obtaining the consumer's consent or, in the case of processing of personal data concerning a known child or student, without obtaining consent from the child's or student's parent or lawful guardian. CPA defines "sensitive data" as:</p> <ul style="list-style-type: none"> <li>• Personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status,</li> <li>• Genetic or biometric data that may be processed for the purpose of uniquely identifying an individual, or</li> <li>• Personal data from a known child.</li> </ul>	SB 6 goes beyond the CCPA by requiring opt-in consent for those under 16 years of age for not only the sale of data (which CCPA requires) but also for targeted advertising and data sales. However, the standard of knowledge is somewhat higher, as it prohibits using an opt-out mechanism when controllers have actual knowledge and willfully disregard that the consumer is at least 13 years of age but younger than 16 years of age.	None

\* indicates that this provision will come into effect January 1, 2023 under CPRA



CCPA



CDPA



CPA



CTDPA



UCPA

**Exemptions**

**Exemptions include:**

- Compliance with the law
- Deidentified or aggregate data
- PHI governed by HIPAA
- GLBA regulated data
- FCRA regulated data
- B2B exemption - personal information collected by a business about an individual consumer, when the consumer is acting as an employee

**Exemptions include:**

- Individuals acting in a commercial or employment context
- Financial institutions subject to GLBA
- Health Care entities HIPAA

CPA does not apply to certain categories of personal data already governed by various state and federal law.

CPA also does not apply to data maintained for employment records purposes. If a business processes personal data pursuant to an exemption under CPA, the business bears the burden of demonstrating that the processing qualifies for the exemption.

Exempts various entities and information types, including certain government entities; covered entities and business associates under HIPAA; information governed by HIPAA; financial institutions or data subject to certain GLBA provisions; nonprofit organizations; institutions of higher education; and personal data regulated by FERPA.

The bill includes broad exemptions for employee data, nonprofits, higher education institutions, covered entities and business associates, personal health information, and GLBA-regulated entities and data, among others.

The consumer rights to access, delete, and obtain a portable copy of data do not apply to "pseudonymous data" (§13-61-303). To qualify as "pseudonymous data" a controller must demonstrate that "any information necessary to identify a consumer" is kept:

- Separately; and
- Subject to appropriate technical and organizational measures to ensure the personal data are not attributed.

Overall, the UCPA includes a number of common exemptions that apply to all provisions of the Act. The Act's requirements "do not restrict a controller or processor's ability" to engage in activities such as:

- Comply with legal obligations
- Cooperate in good faith with law enforcement agencies
- Take action concerning legal claims
- Provide a product or service specifically request by a consumer or perform a contract
- Detect, prevent, protect against, or respond to security incidents or other malicious behavior;
- Conduct internal research for product improvement purposes
- Effectuate a recall
- Identify and repair technical errors
- Perform internal operations reasonably aligned with consumer expectations or otherwise compatible with processing to aid in providing a specifically request product or service; and to protect trade secrets (§ 13-61-304).

The UCPA also exempts from coverage identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. Part 46; identifiable private information that is otherwise information collected as part of human subjects research pursuant to or under the same standards as: (A) the good clinical practice guidelines issued by The International Council for Harmonisation; or (B) the protection of Human Subjects under 21 C.F.R. Parts 50 and Institutional Review Boards under 21 C.F.R. Part 56" (§ 13-61-102(2)(g)).

Finally, the UCPA contains an exception to the Act's requirements for public interest research. The Act provides that the obligations imposed on controllers or processors shall not restrict the ability to "engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws" provided that the processing is disclosed in the controller's transparency notice (§ 13-61-304(1)(j)).

\* indicates that this provision will come into effect January 1, 2023 under CPRA

#### About WireWheel

Founded in 2016 by a team of privacy and technology experts, WireWheel is a leader in the privacy and data protection space. Leveraging the team's deep privacy expertise, WireWheel has developed an easy-to-use platform that enterprises including large financial institutions, telecoms and consumer-facing brands use to manage their privacy programs.

[wirewheel.io](https://www.wirewheel.io)

