

## CHECKLIST

# PRIVACY POLICY

This checklist identifies the key concepts to address in your consumer-facing privacy policy to comply with omnibus consumer privacy laws in the United States, European Union, and Australia. Note that in addition to these privacy policy requirements, some of these laws also require companies to provide additional privacy notices, such as personnel and applicant privacy policies, notices at collection, notices of financial incentives, notices of opt-out rights, and

notices related to the use of cookies, among others. Some laws also impose additional notice obligations on businesses that process certain types of data (e.g., children's data, consumer health data, or biometric data) or sell sensitive data, even if they fall outside typical thresholds for being considered covered entities.

Please consult your Ashurst Perkins Coie privacy lawyer for more information.

## General Information

<input type="checkbox"/>	Company contact information	Provide the business name under which a company is registered and any additional business name(s) the company uses. Include contact information, such as an email address or another online contact method, for consumers to direct their privacy-related questions or concerns.
<input type="checkbox"/>	Notice of changes	Reserve the ability to make updates to the privacy policy. Address the concept of providing notice and obtaining consent in the event of material changes to the policy.
<input type="checkbox"/>	Date of last update	Some laws require an annual update to the privacy policy. Even where this is not required, it is best practice to regularly review and update your privacy policy to ensure it accurately and comprehensively reflects your company's practices.
<input type="checkbox"/>	Accessibility requirements	Companies should strive to meet accessibility standards for all consumers with disabilities, regardless of jurisdiction.
<input type="checkbox"/>	Formatting	Companies must present information in an easy-to-read and understandable format. Use clear and plain language appropriate for the audience and avoid technical or legal jargon.

# Description of Company's Information Practices

---

<input type="checkbox"/>	Collection of PI	Disclose the types and categories of personal information (PI) collected (in the preceding 12 months in California) in a manner that provides consumers with a meaningful understanding of the information being collected. Common categories of PI include identifiers, internet or other electronic network activity information, geolocation information, employment information, and sensitive PI.
<input type="checkbox"/>	Categories of sources from which PI is collected	Some laws require identification of categories of sources from which PI is collected. Examples of categories enumerated in the California Code of Regulations include advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, etc.
<input type="checkbox"/>	Use/purpose(s) of processing	Identify processing purposes in a manner that allows the consumer to understand why PI is collected. Examples of purposes include payment processing, fraud prevention and protection, and delivering products and services requested by the consumer. Some laws require 1:1 matching where a description of the purpose of processing is provided for each category of PI collected.
<input type="checkbox"/>	Disclosures of PI	Identify the categories of PI that the company discloses to a service provider or contractor (in the preceding 12 months in California, or affirmatively state that the company has not made such disclosures in the preceding 12 months). Some laws require that the categories of third-party recipients must be described at a level of detail that enables a consumer to understand the type of third party, business model, or processing conducted by each third party. Companies must also include the specific purpose for disclosing the PI.
<input type="checkbox"/>	Sales/sharing/ targeted advertising	<p>Disclose that the company engages in "<b>selling</b>," "<b>sharing</b>," or "<b>targeted advertising</b>" (or affirmatively state that the company has not engaged in such activities in the preceding 12 months in California) and describe the manner in which a consumer may exercise the right to opt out of such processing. To determine whether your company engages in these activities, disclose the categories of PI that were subject to selling, sharing, or targeted advertising (in the preceding 12 months in California) and the specific categories of third parties to whom the PI was sold or shared. Rhode Island law requires commercial website operators or internet service providers to identify all third parties to whom they have sold, or may sell, customers' "<b>personally identifiable information</b>" (not defined).</p> <p>Companies must also include the purpose for "<b>selling</b>" or "<b>sharing</b>" and a statement regarding whether the company has actual knowledge that it "<b>sells</b>" or "<b>shares</b>" the PI of children (note that state laws have varying age thresholds). If the company sells sensitive data, some states require specific language for the notice, such as "<b>NOTICE: This website may sell your sensitive personal data</b>" or "<b>NOTICE: We may sell your sensitive personal data.</b>"</p> <p>If the company sells biometric data, some states require specific language for the notice, such as "<b>NOTICE: This website may sell your biometric personal data</b>" or "<b>NOTICE: We may sell your biometric personal data.</b>"</p>

---

# Description of Company's Information Practices Continued

<input type="checkbox"/> Automated decision-making or profiling	If the company processes PI for automated decision-making or profiling in furtherance of decisions that produce legal or similarly significant effects, some states require that the policy disclose such processing and inform consumers of their rights related to this processing (e.g., access, opt out, right to challenge).
<input type="checkbox"/> Data retention	Some states require a description of the company's retention policies for PI, including the length of time for which the data will be stored or describe the criteria used for determining such retention period.
<input type="checkbox"/> Sensitive PI	If the company processes sensitive PI (e.g., racial or ethnic origin, biometric data, precise geolocation data, consumer health data, and personal data collected from minors, among others), the privacy policy should disclose the types of sensitive PI processed, purpose(s) for processing the sensitive PI, whether such information is sold or shared with third parties, how consumers can exercise their rights with respect to such data, and retention periods.
<input type="checkbox"/> Financial incentive/ bona fide loyalty program	If a company provides financial incentives or bona fide loyalty programs, the privacy policy should provide notice of the material terms of the incentive or program, how the consumer can opt in and withdraw, the categories of personal data collected through the program, how such data will be sold or shared, and in some cases a good faith estimate of the value of the consumer's data, among other things.



# Consumer Rights & Choices

<input type="checkbox"/> Consumer privacy rights	<p>Notify consumers of the rights and choices available to them under applicable law (e.g., rights to access; correct and delete PI; opt out of sales, sharing, targeted advertising, profiling, and automated decision-making; challenge profiling results; access information regarding use of profiling and automated decision-making technology; know third-party recipients).</p>
<input type="checkbox"/> Nondiscrimination/ no retaliation	<p>State that the company will not discriminate or retaliate against the consumer for exercising any privacy rights, including when a consumer is an applicant to an educational program, a job applicant, a student, an employee, or an independent contractor.</p>
<input type="checkbox"/> Instructions for exercising rights	<p>Precise requirements vary across these laws, but companies should generally designate two or more methods for submitting requests. Some states require that companies list the procedures for an authorized agent to submit a request on a consumer's behalf, describe the process used to authenticate the identity of a consumer or authority of an authorized agent exercising a request, and explain how requests using universal opt-out mechanisms will be processed, among other things.</p>
<input type="checkbox"/> Instructions for appeal	<p>Provide instructions on how a consumer may appeal the company's action in response to a consumer request.</p>
<input type="checkbox"/> Formatting	<p>Companies must present information in an easy-to-read and understandable format. Use clear and plain language appropriate for the audience and avoid technical or legal jargon.</p>

# Additional Australia Requirements

<input type="checkbox"/> Consumers interacting without identifying themselves	<p>If practical, a consumer must be able to interact with the company either without identifying themselves or by using a pseudonym. If it is practical to offer this option, consumers should be made aware, usually in a privacy policy.</p>
<input type="checkbox"/> International data transfers	<p>State whether the company is likely to disclose PI to a person outside of Australia, and if practicable identify relevant countries. Australia's privacy laws can extend to PI that is physically collected or generated outside of Australia, so this requirement is not limited to PI physically transferred out of Australia.</p>
<input type="checkbox"/> How personal information is held, stored, and secured	<p>Explain how the entity holds PI, not just how it collects and discloses it. This should include how PI is stored and secured (e.g., if it is held by a data storage or cloud service provider).</p>
<input type="checkbox"/> How complaints are handled	<p>Explain how privacy complaints will be handled. This means explaining the company's complaints handling processes, not just how to make a complaint.</p> <p>This should include the procedure and contact details for making complaints to the Office of the Australian Information Commissioner or an external dispute resolution scheme for certain sectors (financial services, utilities, telecommunications, public transport, and tolling).</p>

## Additional EU/European Economic Area (EEA) Requirements

---

<input type="checkbox"/>	Legal basis of processing (GDPR)	Companies that are subject to the General Data Protection Regulation (GDPR) must state the legal bases upon which they rely to process PI. Where a company relies upon legitimate interests, it must explain its interests in the privacy policy.
<input type="checkbox"/>	International data transfers (GDPR)	If a company transfers PI from the EEA to a <b>"third country"</b> that is located outside of the EEA, the company must disclose this fact. Companies must also disclose whether an adequacy decision for such third country is in place, or, if there is not an adequacy decision, companies must disclose the safeguards upon which they rely as a lawful mechanism to facilitate the cross-border transfer and the means by which the consumer may obtain a copy thereof (or where they have been made available).
<input type="checkbox"/>	Whether the consumer is required to provide PI (GDPR)	Under the GDPR, to the extent a data subject is required to provide its PI by virtue of a contractual or statutory commitment, the privacy policy must explain that as well as the consequence of not providing personal information.
<input type="checkbox"/>	Data protection officer and EU representatives (GDPR)	Organizations subject to the GDPR may be required to appoint a data protection officer (DPO) or an EU representative. If applicable, the contact details of the DPO and/or EU representative are required.

---

## Additional US State-Specific Requirements

---

<input type="checkbox"/>	Consumer rights request metrics (CCPA)	Companies that processed the PI of 10 million or more California residents in the previous calendar year must include specific metrics in their privacy policy, such as the number of consumer rights requests made and response times.
<input type="checkbox"/>	Language requirement	Some laws require information to be made available in the language(s) primarily used to interact with the consumer or each language in which the company provides a product or service subject to the notice.
<input type="checkbox"/>	Training large language models	Some states require a statement disclosing whether the controller collects, uses, or sells personal data for the purpose of training large language models.

---

# FOR MORE INFORMATION

Contact us at [PrivacySolutions@ashurstperkins.com](mailto:PrivacySolutions@ashurstperkins.com)

Some jurisdictions in which Ashurst Perkins Coie US LLP practices law may require that this communication be designated as Advertising Materials. © 2026 Ashurst Perkins Coie US LLP

**ASHURST  
PERKINS  
COIE**