

Regulation Questions	Answers			
	<p>The GDPR applies to:</p> <p>Organizations located within the European Union (EU).</p> <p>Organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects.</p> <p>Both controllers and processors, meaning 'clouds' and other data processors are not exempt from GDPR enforcement.</p> <p>Non-profit and charitable organizations as well. Reference: GDPR Article 3</p>			
Who must comply with the GDPR?	<p>Under the GDPR, organizations can be fined up to 4% of their annual global turnover or €20 million (whichever is greater) for the most severe infringements. Lesser infringements can result in a fine of up to 2% of annual global turnover or €10 million.</p>			
What are the GDPR fines?	<p>Reference: GDPR Article 83</p>			
	<p>Compliance can be complex and may vary depending on your specific operations, but some general steps include:</p> <p>Conducting a Data Protection Impact Assessment (DPIA).</p> <p>Appointing a Data Protection Officer (DPO) if necessary.</p> <p>Ensuring you have a lawful basis for processing data.</p> <p>Protecting data using appropriate security measures.</p> <p>Notifying authorities of data breaches within 72 hours.</p> <p>Ensuring data subjects' rights are upheld.</p> <p>Ensuring that data transferred outside the EU is adequately protected.</p> <p>Reference: GDPR - A guide to compliance</p>			
How do I comply with the GDPR?	<p>The GDPR does not mandate specific technologies like encryption. However, it requires organizations to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. For many organizations, this could mean using encryption, especially when transmitting personal data or storing it in vulnerable environments.</p>			
Does the GDPR require encryption?	<p>Reference: GDPR Article 32</p>			
	<p>Personal Data: Any information relating to an identified or identifiable natural person. This can include name, identification number, location data, online identifier, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.</p> <p>Sensitive Personal Data: This encompasses data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.</p>			
What is personal information and sensitive personal information under the GDPR?	<p>Reference: GDPR Article 4 &amp; 9</p>			
	<p>GDPR provides several rights to individuals, including:</p> <p>Right to be informed</p> <p>Right of access</p> <p>Right to rectification</p> <p>Right to erasure (or 'right to be forgotten')</p> <p>Right to restrict processing</p> <p>Right to data portability</p> <p>Right to object</p> <p>Rights in relation to automated decision making and profiling.</p> <p>Reference: GDPR Articles 12-23</p>			
What rights do I have under the GDPR?				
	<p>"Under the CCPA, businesses that collect the personal information of California residents must comply if they meet any of the following criteria:</p> <p>Have gross annual revenues in excess of \$25 million;</p> <p>Buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices;</p> <p>Derive 50% or more of their annual revenues from selling California residents' personal information.</p> <p>Reference: Cal. Civ. Code § 1798.140(c)(1)"</p>			
Who must comply with the CCPA?				

<p><b>What are the CCPA fines?</b></p>	<p>The CCPA establishes two main tiers of fines:</p> <p>For unintentional violations: Civil penalties of up to \$2,500 for each violation.  For intentional violations: Civil penalties of up to \$7,500 for each violation.  Furthermore, the CCPA also provides a private right of action for data breaches. If a breach occurs due to a business's failure to implement reasonable security practices, affected consumers can recover between \$100 and \$750 per incident or actual damages, whichever is greater.</p> <p>Reference: Cal. Civ. Code §§ 1798.155 and 1798.150</p>			
<p><b>How do I comply with the CCPA?</b></p>	<p>Compliance with the CCPA involves various steps, including but not limited to:</p> <p>Informing consumers about the categories of personal information you collect and the purposes for which they will be used.  Providing a clear method for consumers to opt-out of the sale of their personal information.  Respecting consumer rights, such as the right to access, delete, or opt-out.  Establishing procedures to respond to consumer requests within specified timeframes.  Reviewing and updating privacy policies and practices regularly.  Implementing reasonable security measures to protect personal information.</p> <p>Reference: Cal. Civ. Code § 1798.100-1798.199</p>			
<p><b>Does the CCPA require encryption?</b></p>	<p>While the CCPA emphasizes the importance of reasonable security procedures and practices, it does not explicitly mandate encryption. However, encryption is recognized as a best practice in data security and can help businesses avoid legal repercussions following a data breach.</p> <p>Reference: Cal. Civ. Code § 1798.150</p>			
<p><b>What is personal information and sensitive personal information under the CCPA?</b></p>	<p>Under the CCPA:</p> <p>"Personal Information" is 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. This could range from names, addresses, and social security numbers to IP addresses and browsing history if it can be linked to an individual or household.</p> <p>Reference: Cal. Civ. Code § 1798.140(o)</p> <p>The CCPA itself doesn't differentiate "sensitive personal information" from "personal information." However, in other contexts like the CPRA (California Privacy Rights Act, which is set to augment and expand upon the CCPA starting in 2023), there are more specific categories of sensitive personal information that include things like precise geolocation, biometric data, and certain personal characteristics.</p>			
<p><b>What rights do I have under the CCPA?</b></p>	<p>As a California resident, the CCPA grants you several rights, including:</p> <p>The right to know what personal information is collected, used, shared, or sold.  The right to delete personal information held by businesses.  The right to opt-out of the sale of personal information.  The right to non-discrimination in terms of price or service when exercising a privacy right under CCPA.</p> <p>Reference: Cal. Civ. Code § 1798.100-1798.199</p>			