CPRA B2B & HR Overview

Overview

Commenced January 1st, 2023, organizations will need to treat B2B and HR data as they do consumer's personal information, bringing the CPRA more in line with the General Data Protection Regulation (GDPR), which already includes provisions for Employee and B2B data.

In preparation, organizations will need to reconfigure their privacy policies, put the infrastructure in place for access requests, ensure they can facilitate right to deletion requests, and more.

What is the CPRA?

The CPRA extends the CCPA. On top of the regulations in the CCPA, the CPRA gives consumers the right to edit and update personal information that is inaccurate, limit how companies use and disclose data about them amongst other things.

As well as this, companies are required to implement special controls to protect highly sensitive data, such as social security numbers and biometric information.

What are the requirements under the CPRA for HR and B2B data?

The CPRA will require organizations to:

- Craft privacy notices to the standard of the CPRA, including details about the collection and usage of employment related and B2B data
- Honor employee requests with regards to the right to know, right to deletion and right to collection, along with the right to op-out of sale or disclosure of this data for advertising purposes. Note, these rights extend to data collected through employee monitoring software.
- Answer employee questions about where, when, and why their company is using their personally identifiable data.

What is HR and B2B data within the CPRA?

Personal information is defined generally as any data that can be used to identify an individual or be reasonably linked to them. Names, addresses, social security numbers and driver's licenses are all considered personal data.

Within the context of employees and the workplace, the following information will also fall under the CPRA: employment contracts, resumes, biometric data, identification badges, surveillance footage and data used for workforce management.

As a side note, it's worth noting that the CPRA will maintain existing carve-out applications, where it is superseded by other federal state privacy laws, as in the case for HIPAA.

Five steps to meet the requirements of the CPRA

Finding a way to maintain vigilant control over your employee and B2B data is going to need a strategic approach and specialist tools. Here's what you need to do:

1. **Map your data:** You can't protect what you don't know about. It's therefore vital to undertake data mapping to create an accurate, thorough inventory of your employee and business data, and the processes for storing and collecting it.
2. **Amend your data classification policies as needed:** Under the CPRA, HR data is often considered sensitive and therefore requires greater protections. Make sure you align your data classification policies to the definitions outlined in the CPRA.
3. **Update your data processing agreements (DPAs):** You likely work with numerous partners and software vendors who could previously process HR data without the worries of compliance fines, as this information was exempt. You'll need to update your DPAs to ensure that all data processing is lawful under the CPRA.
4. **Be prepared for data subject requests from employees:** You will need to extend your data subject right procedures to include employee data.
5. **Adapt your training programs:** Employees will need to be aware of the CPRA's additional requirements, and how this impacts expectations around interactions with HR and B2B data.

CPRA vs CCPA

	CCPA	CPRA
Threshold Application	For-profit businesses that collect personal information from California residents, determines the purposes in California and meet any of the following: • Have a gross annual revenue of over $25 million; • Buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices; or • Derive 50% or more of their annual revenue from selling California residents' personal information.	For-profit businesses that collect personal information from California residents, determines the purposes in California and meet any of the following: • Have a gross annual revenue of over $25 million; • Buy, sell, or share the personal information of 100,000 or more California residents or households; or • Derive 50% or more of their annual revenue from selling or sharing California residents' personal information.
Employee and B2B Exemption	Expires on Jan. 1, 2021	Expires on Jan 1, 2023
Consumer Rights	• Right to Know/Access • Right to Delete • Right to Opt-out of Sale • Right to Non-Discrimination	All rights under the CCPA, plus: • Right to Rectification • Right to Limit Use and Disclosure of Sensitive Personal Information
Covered Personal Information	"Personal information" means 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.	Personal information, as well as "Sensitive Personal Information" which includes information such as SSN, driver license numbers, biometric information, precise geolocation, and racial and ethnic origin.
Third Parties	"Service Provider" – an entity that processes personal information on behalf of a business pursuant to a written contract.	Also includes "Contractor" – an entity 'to whom a business makes available a consumer's personal Information for a

		business purpose pursuant to a written contract with the business'
Enforcement	• Attorney General can pursue violations • Consumers have a private right of action for a breach of certain information • Businesses have a 30-day cure period before being fined for a violation by the AG	• Creation of the California Privacy Protection Agency for enforcement and guidance • Consumers have a private right of action for a breach of certain information • Businesses no longer have a 30-day cure period before being fined for a violation by the CPPA
Definition – Sell vs. Share	"Sell" – for monetary or other valuable consideration.	• "Sell" – for monetary or other valuable consideration • "Share" – share by a business to a third party for cross-context behavioral advertising for the benefit of a business where no money is exchanged.
Use Limitation	N/A	Collection, retention, and use should be limited to what is necessary to provide goods or service.
Private Right of Action	Available when a consumer's unredacted or unencrypted personal information has been breached due to a lack or maintenance of reasonable security measures.	In addition to unredacted and unencrypted personal information, a private right of action is available if an email address and password or security question and answer that would allow access to the account is breached.
Personal Information of Minors	Fines for violations of the personal information for minors is the same as the fines for other types of personal information – $2,500 for each unintentional and $7,500 for each intentional violation	Automatic $7,500 fine for a violation involving the personal information of minors

Required Cybersecurity Audits	N/A	Annual cybersecurity audit required for businesses whose processing presents a significant risk to consumer privacy or security
Required Risk Assessments	N/A	Businesses whose processing presents a significant risk to consumer privacy or security must submit a regular risk assessment to the CPPA
Profiling and Automated Decision Making	N/A	"Profiling" – any form of automated processing of personal information to evaluate certain personal aspects relating to a natural person, such as work performance, health, reliability, etc. Regulations are expected to give additional information on access and opt-out rights for the use of automated decision making.

Source: IAPP