King & Spalding
Client Alert

Global Human Capital and Compliance

FEBRUARY 9, 2022

For more information, contact:

Thomas Ahlering
+1 312 764 6949
tahlering@kslaw.com

Amanda Sonneborn
+1 312 764 6940
asonneborn@kslaw.com

Matthew Krimski
+1 202 626 8977
mkrimski@kslaw.com

Jinouth Vasquez Santos
+1 213 443 4322
jvasquezsantos@kslaw.com

King & Spalding

Chicago
110 N Wacker Drive
Suite 3800
Chicago, IL 60606
Tel: +1 312 995 6333

Start Aiming Now: Employers Have One Year Left to Ensure Compliance with The California Privacy Rights Act (CPRA)

Series 2, 10 in 10: Issue 5

Effective January 1, 2023, the California Privacy Rights Act ("CPRA"), will expand the California Consumer Privacy Act ("CCPA") by granting employees additional rights over their personal information. Employers will now be subject to new obligations—subject to a pending rulemaking process that will provide further clarity regarding the CPRA's impact in the employment context.

CURRENT OBLIGATIONS UNDER THE CCPA

Employers are currently exempt from most of the regulations and are only required to:

- Notify employees before or at the time employees' personal information is collected. The notice must contain the categories of personal data collected and the purpose(s) of collection.
- Maintain "reasonable" and "appropriate" safeguards to protect employee personal information (enforceable through a private right of action—with maximum statutory damages of up to $750 per individual).

CPRA RIGHTS AND OBLIGATIONS

The CPRA removes the exemption for employment information and imposes the following additional obligations on employers:

- **Notice**. The CPRA expands employers' notice obligations to employees. Employers must also provide details regarding whether personal information has been disclosed and for how long information will be retained.

- **Rights to Know/Access/Portability**. Employees can request, and employers must provide (subject to exceptions), the personal information they collect about the employee during the preceding 12 months provided that the personal information was collected after January 1, 2022. Employees may also request that employers transmit specific pieces of personal information to the employee or another entity.
- **Right to Correct**. Employees can request that employers correct inaccurate personal information.
- **Right to Delete**. Employees can request that employers delete their personal information. However, employers can deny the request and retain personal information: (i) reasonably anticipated by the employee within the context of an ongoing relationship with the employer; (ii) necessary to perform on a contract between the employee and employer; or (iii) needed to comply with a legal obligation. Employers must also notify a third party of its related obligation to delete an employee's personal information.
- **Right to Restrict Use of Sensitive Personal Information**[1]. Employees can: (i) request that employers restrict the use of their sensitive personal information; (ii) direct an employer to limit its use of sensitive personal information to specific business purposes; and (iii) instruct an employer to limit disclosure of sensitive personal information, absent a qualifying exemption.
- **Right to Opt-Out of "Sale" of Personal Information**. Employees can opt-out of the "sale" of personal information. Employers must wait 12 months before asking employees for consent to share or sell their personal information after they opt-out of such use.
- **Right to Access/Opt-Out of Automated Decision Technology**. Employees can request information collected about them through automated decision-making and "profiling" technologies with an explanation of the logic behind the collections. Employees can also opt-out of an employer's use of automated decision-making related to their performance, health, behavior, reliability and location/movement.
- **Audit Obligations**. Employers are required to complete regular risk assessments and cybersecurity audits. Further, the CPRA contemplates regular reporting of the results of these audits.
- **No Discrimination or Retaliation**. The CPRA prohibits discrimination and retaliation against employees who exercise their rights under the CPRA.

CPRA ENFORCEMENT

The CPRA also creates a new enforcement authority—the California Privacy Protection Agency ("CPPA")—which will operate alongside the California Attorney General, who currently oversees California's data privacy laws. The CPPA will have rulemaking, investigative and enforcement powers. Employees can assert a private right of action for actual damages in the data breach context without providing notice and an opportunity to cure. There is, however, a 30-day cure period in which an employer can cure a violation and provide an express written statement that the violation has been cured, to avoid incurring statutory penalties. Finally, a private right of action is limited to the data breach context and is not applicable to other violations of the CPRA.

SUBJECT AREAS FOR FURTHER REGULATION

Regulations implementing the CPRA have not yet been issued. The CPRA directs the CPPA to develop and adopt regulations for over twenty subject areas that further the purposes of the CPRA. Relevant regulations are expected on:

- Definitions, generally, and categories of personal information subject to heightened regulation (terms and concepts subject to additional clarification include: “personal information,” “sensitive personal information,” “unique identifier” (i.e., cookies), “business purposes,” “geolocation,” and “investigation.”);
- Rules and procedures governing employees’ requests to delete, correct, know, access and opt-out of processing (and employers’ responses thereto);
- Standards establishing the when and why employees can make data requests;
- Requirements for employers’ notices to employees, including the specific pieces of information that employers are required to provide;
- Clarification of automated decision-making access and opt-out rights and obligations;
- The frequency, scope and requirements for risk assessments and cybersecurity audits where processing presents a “significant risk to [employee] privacy and safety”; and
- Exceptions to comply with other laws, including, discrimination, trade secrets and intellectual property.

EXEMPTIONS

While most employment-related information is currently excluded, that exemption ends on January 1, 2023. In addition to the broad current exemption, the CPRA also provides the following exemptions potentially applicable in the employment context that could limit the CPRA’s scope:

- Emergency contact information used solely by an employer to have an emergency contact on file;
- Benefits information of individuals related to employees used to administer their benefits;
- Medical information;
- Deidentified and aggregate information provided the employer implements security safeguards;
- Information necessary to comply with law enforcement requests, comply with other applicable laws, and defend against legal claims; and
- Information which is publicly available.

CONCLUSION

The CPRA brings with it significant requirements for employers, which will likely require employers to:

- Developing new procedures to respond to employee requests;
- Data mapping to understand the employee data collected, the categorization of data, the location of the data, and the steps to access, correct or delete the data;
- Determining potential exemptions in the employment context and their applications;
- Revising/implementing retention policies and notices;
- Developing document retention policies and responding to related audits and enforcement actions;
- Reviewing contracts with third parties to include proper safeguard provisions and deletion requests.

King & Spalding will continue to update this guidance as the CPRA regulations are finalized.

[1] The CPRA creates a new, broad category of "sensitive personal information" which is subject to additional requirements. Data under this category includes Social Security numbers, driver's license, state identification card, and passport numbers; financial account numbers in combination with login credentials; account logins with passwords; geolocation information; information about race, ethnicity, religious/philosophical beliefs, and union memberships; and genetic data.