DATA PRIVACY: PREPARING FOR 2023 (AND BEYOND) IN CALIFORNIA – CHILDREN'S PRIVACY, EMPLOYEE AND B2B DATA EXEMPTIONS EXPIRING, AND CPRA COMES INTO FORCE

As 2023 approaches, a flurry of activity in California means big changes in the year ahead for data privacy. New obligations, an expanded scope of covered data, increasing enforcement, and scant regulations all mean it's a good time for companies processing the personal information of California residents to make sure they're prepared for the new year. Read ahead for insights into what's coming and strategies for compliance, including Frequently Asked Questions.

KEY CCPA EXEMPTIONS EXPIRING IN JANUARY 2023

Upon becoming effective in 2020, the California Consumer Privacy Act ("CCPA") temporarily exempted covered entities from complying with most of the CCPA's requirements with respect to personal information related to workforce members and B2B communications. These exemptions last until January 1, 2023. Many expected the exemptions to be renewed, but despite many attempts, legislators were unsuccessful, and the legislative session ended in August without any action. This means companies should expand (or create) their compliance program to cover employee and B2B data.

What types of personal information fall under the employee and B2B exemptions?

The employee exemption covers the personal information of California job applicants, employees, owners, directors, officers, and medical staff members, as defined in the statute, collected and used by businesses in the context of an individual's role, for emergency contact information, or to provide benefits. Until 2023, the law exempted this data from most CCPA obligations, but at collection employers are still required to provide a notice to their employees explaining what information is being collected and its intended use.

The B2B exemption covers personal information reflecting a written or verbal communication or transaction between a covered business and an employee, owner, director, officer, or independent contractor, of another business, which

occurs within the context of conducting due diligence or providing or receiving a product or service. Until 2023, the law only requires B2B data to be subject to the statute's personal information sales opt-out and opt-in rights, non-discrimination obligations, and private right of action for data breaches.

These exemptions expire on January 1, 2023, after which this data will be subject to all aspects of the CCPA, as amended by the California Privacy Rights Act ("CPRA"), just like any other personal information of California residents.

FAQ 1: How can companies prepare to comply with the expanded scope of the CCPA and CPRA?

Companies who are already compliant with the CCPA should have many of their processes and policies in place; their main tasks will be to update their notices, policies, and processes to include employee and B2B personal information (in addition to refreshing the policies to comply with the expanded requirements of the CPRA—see below). In particular, companies should consider how to handle employee data requests in light of employment laws and existing HR policies. Many companies are configuring their HR portal to permit employees to exercise their rights without requiring a separate request.

Meanwhile, global companies that must comply with the European Union's General Data Protection Regulation ("GDPR")—which has none of these exemptions—can draw upon their experience handling this data under their GDPR policies and procedures.

As for entities which are new to these obligations, they should start now to set up policies and procedures to avoid scrambling as 2023 approaches.

Some steps to prepare for compliance include:

- Conducting a thorough assessment of how employee (including applicants') and B2B personal information is currently collected, used, and disclosed, including what categories of personal information are involved and to what extent data minimization protocols should be put in place
- Supplementing privacy notices to ensure they include information regarding data subject's rights with respect to this previously exempted information
- Expanding existing policies and procedures regarding the retention of personal information and handling CPRA rights requests (right to know, delete, etc.) to incorporate employee and B2B-related requests
- Assessing contracts with relevant service providers and businesses which have access to employee and B2B data to ensure downstream compliance and, if applicable, the inclusion of clauses required for those businesses to remain service providers.

AGE-APPROPRIATE DESIGN LEGISLATION

Following in the footsteps of Europe's Age-Appropriate Design Code enacted in 2020, California enacted the California Age-Appropriate Design Code Act ("CAADCA") on September 15, 2022. Under the CAADCA, online platforms must

"consider the best interests of children when designing, developing, and providing that online service, product, or feature." Businesses also must prioritize children's safety and well-being wherever there is a conflict between their commercial interests and the interests of children who access these platforms. The CAADCA is scheduled to come into force on July 1, 2024, although some obligations kick in earlier.

Who is covered by the statute?

The CAADCA applies to any business that "provides an online service, product, or feature likely to be accessed by children" under the age of 18. Terms not defined in the legislation follow the CCPA's definitions, as amended by the CPRA. Therefore, "business" under the CAADCA has the same meaning as under the CCPA/CPRA, which includes any for-profit entity doing business in California that collects personal information of California residents and meets one or more specific thresholds defined by the statute.

The CAADCA provides several factors for determining whether a product, service, or feature is one that is "likely to be accessed by children," including:

- whether it is directed to children as defined by the Children's Online Privacy Protection Act ("COPPA," a federal children's privacy law)
- whether it is determined to be routinely accessed by a significant number of children according to competent, reliable evidence
- whether its advertisements market to children
- whether it has design elements that are known to be interesting to children, including games, cartoons, music, and celebrities that children enjoy.

FAQ 2: What are some of the key obligations under the CAADCA?

The law imposes a set of obligations on covered businesses, including:

- **Data Impact Assessments:** Covered businesses must complete a "Data Protection Impact Assessment" before offering any new online service, product, or feature, to the public that is likely to be accessed by children. The assessment should analyze and explore mitigations for any potential risk to children, such as whether algorithms used in a product or advertisements displayed could be harmful to children. These assessments must be made available within three business days of a request from the California Attorney General. Importantly, a Data Impact Assessment must be completed on or before the effective date of the CAADCA—July 1, 2024—for any online service, product, or feature likely to be accessed by children and offered to the public before July 1, 2024 and after.
- **Default privacy settings**: All default privacy settings of online services, products, or features, provided to children must be configured in such a manner as to provide a high level of privacy, unless the business has a compelling reason that a different privacy setting is in the best interests of children.

- **Prominently and easily display privacy information**: All privacy policies, terms of service, and community standards information must be concise and prominently displayed with language suitable for the age of children likely to access the online program. Companies also must clearly notify children if their activity is being monitored or tracked, even if by a parent or guardian.
- **Various restrictions to keep children safe**: All covered businesses are prohibited from (i) using personal information of children in a way that is detrimental to a child's well-being, (ii) profiling a child unless necessary to provide the online service or feature, or if the business has a compelling reason that that is in the best interests of the child, (iii) collecting, selling, or disclosing, precise geolocation data unless strictly necessary, and (iv) using dark patterns—a deceptive design pattern—to entice children to provide their personal information.

FAQ 3: How will the CAADCA be enforced?

Any business that violates the CAADCA will be subject to an injunction and civil penalty of no more than $2,500 per affected child for each negligent violation and no more than $7,500 for each intentional violation. These enforcement actions may be brought by the California Attorney General.

CPRA OBLIGATIONS FINALLY COME INTO EFFECT

Next year brings other key changes to data protection in California, with many of the substantive provisions of the CPRA coming into effect, including:

- Expanding the definition of business to companies who derive over 50% of their annual revenues from "sharing" personal information;
- A new consumer right to correct inaccurate personal information;
- Definition (and limitations on use) of "sensitive" personal information;
- Expanded rights and obligations, including disclosure of retention limits, data and purpose limitation obligations, and reasonable security measure obligations; and
- Expanded contractual requirements for agreements with service providers and contractors.

Companies should take this opportunity to review their policies and procedures to ensure compliance with these expanded obligations. Because the CPRA regulations have not been finalized, companies should also remain alert to communications from the California Office of the Attorney General and California Privacy Protection Agency ("CPPA"). For example, on October 17, 2022, the CPPA published proposed modifications to the CPRA regulations that seek to clarify some of the key obligations. To receive notifications on CCPA and CPRA-related developments, sign up here: https://oag.ca.gov/subscribe.

CONCLUSION

There is mounting evidence that enforcement of California privacy laws will increase in 2023. Earlier this month, the California Attorney General issued its first monetary penalty for CCPA violations—a $1.2 million action against Sephora

for noncompliance with obligations (see our article here for more details). Along with the penalty, the AG announced new enforcement sweeps, including against financial institutions and large consumer retailers. Meanwhile the state continues to build out its new privacy regulator, the California Privacy Protection Agency, complete with a $10 million/year operating budget. In addition, the mandatory 30-day cure period for noncompliance becomes discretionary in 2023—meaning the CPPA or AG can go directly to enforcement if they determine that that is appropriate.

And that's just California! The Virginia CDPA comes into effect on the same day (see our briefing here), with Colorado (see here) and Connecticut (see here) appearing shortly afterwards, followed by Utah (see here) at the end of 2023. And with the looming specter of a comprehensive national privacy bill (see our discussion here), it will be more important than ever for companies to have thorough data privacy and governance protocols in place.

CONTACTS

Devika Kornbacher
Partner

T +1 212 878 3424
E devika.kornbacher
@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Shannon O'Brien
Associate

T +1 212 880 5709
E shannon.obrien
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.