The impact of the American Data Privacy and Protection Act (ADPPA) to B2B businesses

January 2023 | Copyright © 2023 | author: Roger Kai

Introduction

ADPPA is probably the most high-profile data protection bill in the U.S. It is proposed to not only provide a national level of data protection framework but also deliver straightforward methods for consumer privacy protection. Therefore, businesses must keep track of ADPPA's development and the possible impact it might bring them on.

What is the impact of ADPPA on B2B businesses? Considering the lack of a new bill to prolong the exemption period for B2B businesses in CCPA and CPRA, the room for taking a breath under the strict data privacy regulation will no longer be available for B2B businesses. The same thing goes for ADPPA; other than employee data in certain scenarios and small businesses exemption, there is no exclusion for personal information under B2B business operations.

The following analysis regarding ADPPA is based on the version amended on December 30, 2022.[1]

The definition of B2B businesses

According to California Civil Code 1798.145(n), the definition for B2B businesses operation refers to "written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit, or government agency."

Businesses that fit into the B2B exemption are exempt from providing notice of the collection, means for exercising consumer rights, and the consumer does not have a right to delete or receive information.

This exemption of CCPA, however, is about to reach an end. As the California legislative session ends in August without any bill to extend the inoperative date, the exemption for B2B, along with employee data, will end on January 1, 2023.

The status of ADPPA

As for ADPPA, there's no specific exemption for data processed by B2B businesses. Therefore, we should look closely at the impact ADPPA might brought.

ADPPA is similar to GDPR in several contexts. First, it provides fundamental principles for privacy protection like transparency, data minimization, data portability, and privacy by design. Secondly, it also set up the rights for individuals to access, correct, and delete covered data. However, there are key differences between the two. Examples of these differences include:

---

[1] American Data Privacy and Protection Act (ADPPA), H.R. 8152, 117th Cong. §2 (2022). https://www.congress.gov/bill/117th-congress/house-bill/8152/text

1. Unlike controller under the jurisdiction of GDPR will be held responsible for the data protection breach of its service providers, in ADPPA, the obligation of cover entities (controller) ceased after transferring the data to service providers if the cover entity is in compliance with ADPPA and have no actual knowledge during the transmission that the service provider would violate it. (Sec. 302 (c) (3))

2. Unlike the exterritorial effect GPDR possess, ADPPA focuses on the data protection of individual residing in the United States and has no additional requirement for international data transfers (ADPPA Sec. 2 (19))

3. In general, there is no requirement for cover entities to conduct DPIA, with the exception of large data holders (see below for further details)

Although ADPPA does not provide an exemption for B2B businesses, some of the businesses might fit in another exemption for small businesses. In ADPPA, small businesses are exempt from the followings (Sec. 209 (a)):

1. Exempt from the data portability requirement. Moreover, small businesses may choose to delete rather than correct the covered data when being requested by individuals.

2. Exempt from specific requirements of data security practices, including vulnerability assessment, taking and evaluating preventive and corrective action, training, Incident response, and the designation of the privacy officer.

3. When individuals seek any relief against small businesses, small businesses have a limited right to cure the alleged deficiency. (Sec. 403 (c))

4. After the enactment of ADPPA, if small businesses find the technical compliance programs FTC promulgated too strict, they are allowed to apply to FTC to approve its compliance guidelines. (Sec. 304(a))

To meet the definition of small businesses, an entity must establish that (Sec. 209 (b)):

1. For the period of the previous three years, its average annual gross revenues do not exceed $41,000,000; and

2. On average, it did not annually collect or process the covered data of more than 200,000 individuals during the period beyond the purpose of initiating, rendering, billing for, finalizing, completing or otherwise collecting payment for a requested service or product. Such data must also be deleted or de-identified within 90 days.

3. It did not derive more than 50 percent of its revenue from transferring covered data during any year.

On the other hand, if businesses fall into the definition of "Large Data Holder," they will face much stricter rules. See below for some of examples:

1. Compiling metric reporting for each calendar year disclosing including but not limited to the number of requests for access, deletion, opt-out from individuals, and whether Large Data Holder complied or denied the requests. (Sec. 203 (f))

2. Lesser time (45 days) to process requests from individuals regarding access, correction, deletion, and portability, with a specific exception for impracticability. (Sec. 203 (c))

3. The obligation to certify to the Commission that it maintains a certain level of internal controls and internal reporting structures.

4. The obligation to conduct data protection impact assessment (DPIA) (Sec.301 (d))

5. Stricter responsibilities for privacy officer/data security officer, including but not limited to maintaining processes for periodic review and policies update, developing employee training programs, and conducting biennial audits to ensure the compliance of the policies, practices, and procedures. (Sec. 301(c))

Large Data Holder defines a covered entity that, subject to exceptions, in the most recent calendar year (Sec. 2 (21)):

1. Had annual gross revenues of $250,000,000 or more; and

2. Collected, processed, or transferred the covered data of more than 5,000,000 individuals or devices or the sensitive covered data of more than 200,000 individuals or devices.

Conclusion

As CPRA's expiration date for B2B exemption reaches its end, B2B businesses may have to prepare themselves for a full stack of privacy regulations, which include ADPPA. However, considering the impact strict privacy regulation may bring to small businesses, ADPPA does provide exemptions for them subject to specific conditions. On the other hand, big companies should be aware of the new rules in ADPPA for large data holders, as they need to follow additional and stricter requirements of ADPPA.

Although ADPPA is still under the voting processes and has lots of potential variants, it is essential to be prepared for the following unified data privacy regulation across the States.

Contact us

For further information on the ADPPA and data privacy, please do not hesitate to contact us!

Robert Niedermeier: niedermeier@db5.io or Severine Petersen: petersen@db5.io