Overview of the American Data Privacy and Protection Act (ADPPA)

- Author: Roger Kai -

Introduction

On December 30, 2022, the U.S. House of Representatives Committee on Energy and Commerce amended and reported the American Data Privacy and Protection Act (ADPPA)[1], which has been placed on the Union Calendar for the further consideration process. If the bill passes the vote, it will proceed to Senate for a series of voting. Generally speaking, there is still a long way for the bill to reach the public.

The following overview is based on the new version of the ADPPA, amended on December 30, 2022.[2]

Key elements

The ADPPA intends to create a unified privacy rule across the countries. Some key elements of the law are as follows:

1) Covered entity: ADPPA would apply to "any entity that collects, processes, or transfers covered data and is subject to the jurisdiction of the Federal Trade Commission (FTC), including nonprofits and telecommunications common carriers." Furthermore, ADPPA distinguishes large data holders and small and medium-sized enterprises.

    a) Large Data Holder: except for certain exceptions, a covered entity that, in the most recent calendar year

        i) Had annual gross revenues of $250,000,000 or more; and

        ii) 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.

    b) Small Business: to meet the definition of small data, an entity must establish that:

---

[1] Gilad Edelman, *Don't look now, but Congress might pass an actually good privacy bill*, WIRED, available at https://www.wired.com/story/american-data-privacy-protection-act-adppa/ (last visited Oct. 18, 2022)
[2] American Data Privacy and Protection Act (ADPPA), H.R. 8152, 117th Cong. §2 (2022). https://www.congress.gov/117/bills/hr8152/BILLS-117hr8152rh.pdf

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

      ii)   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.

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

2) Covered data: ADPPA would apply to any information that is linked or reasonably linkable to an individual or a device that is reasonably linkable to one or more individuals. (Including unique identifiers, like IP address and cookies). Moreover, ADPPA defined certain kinds of data as "sensitive covered data," which are subject to heightened requirements. Finally, the following data are excluded from ADPPA: de-identified data, employee data, and publicly available information.

3) Duty of Loyalty

    a)   ADPPA would impose several duties on covered entities, including privacy by design and data minimization. Furthermore, it would restrict covered entities from engaging in certain data practices, including but not limited to transferring biometric and genetic information, aggregated internet browsing and search history, and physical activity information.

    b)   Despite ADPPA having thoroughly listed the specific items that might endanger cover entities' duty to individuals. ADPPA does not prohibit general provisions for potential harmful practices that the law did not foresee and list.

4) Transparency

    a)   ADPPA would require covered entities to provide individuals with privacy policies detailing how they collect, process, and transfer the covered data and their security activities in a readily available and understandable manner.

    b)   Notably, covered entities must disclose if any covered data collected by them are made available to the People's Republic of China, Russia, Iran, or North Korea.

5) Consumer Control and Consent: ADPPA would give consumers several rights to their covered data, including the right to access, correct, and delete their data held by a covered entity.

6) Youth Protection: In Children's Online Privacy Protection Act of 1998 (COPPA), the law only targets children under the age of 13. However, ADPPA would set different levels of standards for children under the age of 13 and the ones between the ages of 13 and 17. Furthermore, ADPPA would require the establishment of Youth Privacy and Marketing Division in FTC, which shall be responsible for privacy concerns relating to children and minors.

7) Discrimination

a) ADPPA would restrict covered entities from collecting, processing, or transferring covered data in a manner that discriminates based on race, color, religion…etc. This includes requiring large data holders to assess their algorithms annually and submit annual assessments to the FTC.

b) The algorithmic evaluation must be conducted at the design phase of an algorithm, including any training data that is used to develop the algorithm.

8) Small business (Small and medium-sized enterprises) protection: if such enterprises meet the definition of small data, as mentioned above, they are exempt from the followings:

a) Exempt from the data portability requirement. Moreover, SMEs may choose to delete rather than correct the covered data when being requested by individuals.

b) Exempt from certain 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.

c) When individuals seek any relief against small and medium-sized covered entities, those entities have a limited right to cure the alleged deficiency.

d) If finding the technical compliance programs FTC promulgated after the enactment of ADPPA too strict, SMEs are allowed to apply for FTC to approve its compliance guidelines.

9) Enforcement: Violations of ADPPA will be treated as violations of a rule defining an unfair or deceptive act or practice under the FTC Act.

10) Private right of action: Two years after ADPPA's enactment, individuals would have a private right of action to sue covered entities for damages, injunction, litigation costs, and attorneys' fees. Individuals would have to notify the FTC or the state attorney general before bringing suit.

11) Preemption: ADPPA would generally preempt state laws that are covered by ADPPA's provisions with a list of exceptions. The exceptions include but are not limited to consumer protection laws of general applicability, data breach notification laws, contract and tort laws, the Illinois Biometric and Genetic Information Privacy Act, and Section 1798.150 of the California Civil Code. As for CCPA, according to the draft, California Privacy Protection Agency may enforce ADDPA in the same manner, it would to implement otherwise the CCPA.

Impact on small and medium-sized enterprises (SMEs) in the USA

Despite ADPPA providing a series of exceptions for SMEs to lower their pressure on privacy compliance costs, ADPPA does intend to regulate SMEs. Once ADPPA becomes effective, SMEs inevitably have to follow a certain level of privacy rules like transparency, data protection for children and minors, and a wide range of personal data protection. However, many sections, like data minimization and privacy by design, still require FTC to provide further guidance; therefore, it remains unclear what the real impact ADPPA will cause.

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

www.data-business-services.com