NISHIMURA & ASAHI

西村あさひ法律事務所

米国個人情報保護法最新動向
ADPPA Bill の概要(10) 企業の説明責任(1)

北米 / 個人情報保護・データ保護規制ニューズレター　2022 年 11 月 10 日

執筆者:
E-mail 石川 智也　E-mail 河合 優子
E-mail 久保 慶太郎　E-mail 水谷 有希

本連載は、米国版 GDPR とも呼ばれることのある、米国の連邦レベルでの個人情報保護法である American Data Privacy and Protection Act (ADPPA)の案について、個別の規定を紹介することを目的とする。第 10 回～第 12 回では、企業の説明責任(Corporate Accountability)について紹介する。本号では、企業の説明責任として定められている規定の概要を紹介した上で、そのうち、経営者責任(Executive responsibility)について紹介する。その他の規定の詳細については、次号以下を参照されたい。

なお、ADPPA の案の全体像や今後の見込みについては、本ニューズレター2022 年 6 月 6 日号や同 7 月 22 日号をご参照いただきたい。また、本連載では、2022 年 7 月 20 日に下院に提出された条文を参照しているが、条文は今後も変更の可能性があるため、参照に当たっては、随時最新の内容であるか慎重に確認されたい。

IV 企業の説明責任(Corporate Accountability)

1. 概要

ADPPA は、第 3 編において、企業の説明責任(Corporate Accountability)として、経営者責任(Executive responsibility)、サービスプロバイダ及び第三者(Service providers and third parties)、技術遵守プログラム(Technical compliance programs)、FTC が承認するコンプライアンスガイドライン(Commission approved compliance guidelines)、デジタルコンテンツの偽造(Digital content forgeries)について定めている。

条　文	概　要
経営者責任(Executive responsibility)(301 条)	FTC に対する毎年の内部統制・内部報告体制の証明、プライバシー・データセキュリティに係るオフィサーの任命、プライバシー影響評価の実施等の義務等が規定されている。
サービスプロバイダ及び第三者(Service providers and third parties)(302 条)	「サービスプロバイダ」及び「第三者」における義務、データ処理の範囲、並びに対象事業体がサービスプロバイダ・第三者を起用する際の追加的義務等が規定されている。
技術遵守プログラム(Technical compliance programs)(303 条)	対象事業体が対象データの収集、処理又は移転のために使用する技術遵守プログラムについて、ADPPA の施行から 3 年以内に FTC が提案及び承認のプロセスを確立する規則を公布する旨、並びに技術的遵守プログラムに対する対象事業体等の承認・修正・廃止要求の提出権等が規定されている。
FTC が承認するコンプライアンスガイドライン(Commission approved compliance guidelines)(304 条)	小規模事業者に該当する対象事業体(第三者収集機関であるものを除く)は、FTC に対して、対象データの収集、処理、移転を規律するコンプライアンスガイドラインの承認を申請することができ、FTC によって承認されたガイドラインを遵守する対象事業体は ADPPA 上の関連規定を遵守しているものとみなされる旨等が規定されている。

デジタルコンテンツの偽造(Digital content forgeries)(305 条)	商務長官(the Secretary of Commerce)がデジタルコンテンツ偽造に関する報告書を毎年公表する旨等が規定されている。

2. 経営者責任(Executive responsibility)

(1) FTC への証明

大規模データ保有者[1]の役員(executive officer)は、ADPPA の成立日の 1 年後から毎年、FTC が定める方法により、FTC に対して証明書(certification)を提出することによって、以下の(i)及び(ii)を証明しなければならない(301 条(a))。

(i) ADPPA を遵守するよう合理的に設計された内部統制が維持されていること
(ii) 当該大規模データ保有者の ADPPA の遵守に影響を与える決定に当該役員が関与し責任を負うことを確保する、内部報告体制が維持されていること

なお、当該証明書は、その提出前 90 日以内に当該役員が行った、当該大規模データ保有者の内部統制及び内部報告体制の有効性に関するレビューに基づいていなければならない。また、当該証明書は、当該役員が、合理的な調査を実施した後、当該証明書の提出時点において、当該証明書に記載された内容は真実であり、かつ、当該証明書に記載する必要のある重要な事実や当該証明書の記載を誤解のないものとするのに必要な重要な事実について遺漏はないと信じ、かつ、そのように信じるに足る合理的な根拠を有している場合に、誠実に作成されたものとされる(301 条(b))。

(2) プライバシー・データセキュリティに係るオフィサーの任命

15 人以上の従業員を雇用する対象事業体又はサービスプロバイダは、その従業員の中から以下のオフィサーをそれぞれ任命しなければならない(301 条(c)(1))。

(a) 1 名以上のプライバシーオフィサー(privacy officer(s))
(b) (上記(a)のプライバシーオフィサーとは別に)1 名以上のデータセキュリティオフィサー(data security officer(s))

プライバシーオフィサー及びデータセキュリティオフィサーは、少なくとも以下に従事しなければならない(301 条(c)(2))。

(i) ADPPA 上の要件に従い、対象データのプライバシー及びセキュリティを保護するために、データプライバシー・プログラム及びデータセキュリティ・プログラムを実施すること
(ii) 対象事業体又はサービスプロバイダにおける ADPPA の継続的な遵守を促進すること

大規模データ保有者には追加の義務が課されている。すなわち、大規模データ保有者は、プライバシーオフィサー又はデータセキュリティオフィサーに任命した従業員の中から少なくとも 1 名を、大規模データ保有者の最高責任者(highest official)に直属するプライバシープロテクションオフィサー(privacy protection officer)に任命しなければならず、プライバシープロテクションオフィサーは、上記(i)(ii)に加え、自ら直接に又は監督下にある者を介して、以下に従事しなければならない(301 条(c)(3))。

(iii) 必要に応じて、大規模データ保有者のプライバシー及びセキュリティに関する方針、実務及び手続を定期的に見直し、更新する手続を定めること
(iv) 大規模データ保有者の方針、実務及び手続が当該大規模データ保持者における ADPPA の遵守を担保していることを確保するために、2 年に 1 回、包括的な監査を実施すること、並びに FTC が要求した場合には当該監査にアクセス可能とすること
(v) ADPPA の遵守に関する従業員教育のプログラムを策定すること
(vi) 大規模データ保有者が行った全ての重要なプライバシー及びデータセキュリティに関する実務について、最新かつ正

[1] 大規模データ保有者の詳細については、本ニューズレター2022 年 11 月 9 日号ご参照。

確な、明快で理解しやすい記録を保持すること

(vii) 大規模データ保有者と執行当局との間の連絡窓口を務めること

(3) プライバシー影響評価

ADPPA においては、大規模データ保有者と、その他の対象事業体とで区別してプライバシー影響評価の実施義務が規定されている。両者の主な違いは、大規模データ保有者は、個人のプライバシーへの悪影響とデータ処理によって得られる利益との比較衡量を行うことが求められるのに対して、その他の対象事業体は、プライバシーへの悪影響のうち重大なものとデータ処理によって得られる利益との比較衡量を行うことが求められる。また、大規模データ保有者は、プライバシーリスクの評価に際し、対象データの安全性を確保するために使用される技術的手段についてのレビューが必要であるが、その他の対象事業体は、かかるレビューも併せて行うことができるとされるにとどまり、かかるレビューは必須でない。それぞれ、詳細は以下のとおりである。

(A) 大規模データ保有者におけるプライバシー影響評価(301 条(d))

大規模データ保有者である対象事業体は、ADPPA の成立から 1 年が経過する日又は当該対象事業体が大規模データ保有者に該当することとなってから 1 年が経過する日のいずれか早い方の日までに、及びその後 2 年毎に、当該大規模データ保有者による対象データの収集、処理、移転のプラクティスによって得られる利益(benefit)と当該プラクティスが個人のプライバシーに与える可能性のある悪影響(重大なプライバシーリスクを含む)とを比較検討するプライバシー影響評価を実施しなければならない。

なお、このプライバシー影響評価は、以下の条件を全て満たさなければならない。

① 当該大規模データ保有者によって収集、処理、移転される対象データの性質及び量、並びに当該大規模データ保有者による対象データの収集、処理、移転によって引き起こされる可能性のある、個人のプライバシーに対する重大なリスクを踏まえて、合理的かつ適切なスコープであること
② 書面化され、その後実施されるプライバシー影響評価によって古いものとなるまで大規模データ保有者において保管されること
③ (該当する場合)当該大規模データ保有者が指定したプライバシープロテクションオフィサーによって承認されていること

また、大規模データ保有者は、プライバシーリスク(重大なプライバシーリスクを含む)を評価する際には、対象データの安全性を確保するために使用される技術的手段(ブロックチェーンや分散型台帳技術、その他の新規技術を含む)についてのレビューも併せて行わなければならない。

(B) その他の対象事業体(小規模事業者を除く)におけるプライバシー影響評価(301 条(e))

大規模データ保有者ではなく、かつ 209 条の小規模事業者[2]にも該当しない対象事業体は、ADPPA の成立から 1 年以内に、及びその後 2 年毎に、重大なプライバシーリスクを生じさせる可能性のある、当該対象事業体による対象データの収集、処理、移転のプラクティスによって得られた利益(benefit)と当該プラクティスが個人のプライバシーに与える可能性のある重大な悪影響とを比較検討するプライバシー影響評価を実施しなければならない。

なお、このプライバシー影響評価は、以下の条件を全て満たさなければならない。

① 当該対象事業体によって収集、処理、移転される対象データの性質及び量、並びに当該対象事業体による対象データの収集、処理、移転によって引き起こされる可能性のある、個人のプライバシーに対するリスクを踏まえて、合理的かつ適切なスコープであること
② 書面化され、その後実施されるプライバシー影響評価によって古いものとなるまで当該対象事業体において保管され

2 小規模事業者の詳細については、本ニューズレター2022 年 9 月 8 日号ご参照。

ること

また、大規模データ保有者又は 209 条の小規模事業者のいずれにも該当しない対象事業体におけるプライバシー影響評価については、プライバシーリスク(重大なプライバシーリスクを含む)を評価する際には、対象データの安全性を確保するために使用される技術的手段(ブロックチェーンや分散型台帳技術、その他の新規技術を含む)についてのレビューも併せて行うことができる旨規定されている。

GDPR35 条においてもデータ保護影響評価の実施が義務付けられている(但し、その実施の義務は、自然人の権利及び自由に高いリスクをもたらす可能性が高い場合(例えばプロファイリングやセンシティブデータ、犯罪に関する個人のデータの大規模処理等を行う場合)に限定されている)。また、CPRA1798.185 条においても、プライバシー影響評価の実施について、今後司法長官が規則を定める旨規定されている。各国のデータ保護法の間で、盛り込むべき事項や論証するべき事項が微妙に異なる中で、どのように各国の要件を充足するように影響評価を実施していくべきかについては、今後の新たな課題であるといえよう。

西村あさひ法律事務所　広報室　E-mail