

地域	テキサス州
日付	2022年4月20日
法律事務所	Polsinelli (https://www.polsinelli.com/)
役職名、氏名	Elizabeth (Liz) Harding, Shareholder Allison Krause, Associate
連絡先	eharding@polsinelli.com , akrause@polsinelli.com

質問事項

I. 個人情報保護に関する法律

- i. あなたの国には、現在又は近い将来施行される予定の私的分野における個人情報保護に関する一般法はありますか。
- ii. あなたの国には、現在又は近い将来施行される予定の公的分野における個人情報保護に関する一般法はありますか。
- iii. あなたの国には、現在又は近い将来施行される予定の個別の(特定の)分野に適用のある個人情報保護に関する法律はありますか。(ある場合は概要を教えてください。)

テキサス州には、個人情報保護に関する包括的な法律はありません。しかし、2007年に、テキサス州は、データ侵害通知法である *Tex. Bus. & Com. Code § 521.002*, 改正後の *521.053*, (以下「TDBA」といいます。)を制定しました。TDBAは、データセキュリティ侵害の通知に関する他の多くの米国の州法と類似しています。さらに、州機関はTDBAの直接の適用対象ではありませんが、*Tex. Govt. Code § 2054.1125* (以下「TGDBA」といいます。)は、テキサス州のすべての州機関に適用され、TDBAの要件を盛り込んでいます。本報告書では、特に断りのない限り、TDBAにはTDBAが含まれるものとして扱います。

Iの(i)(ii)(iii)について全て「該当なし」の場合はIVに進みます。

II. 個人情報の保護に関する規程の基本情報

- i. Iで言及いただいた個人情報保護に関する法律全てについて以下の空欄を埋めて下さい(必要に応じて回答欄を追加してください。)

名称: *Tex. Bus. & Com. Code*

URL: <https://statutes.capitol.texas.gov/Docs/BC/htm/BC.521.htm#521.053>

施行状況: 2009年4月1日制定、2012年9月1日・2013年6月14日・2020年1月1

日・2021年9月1日改正

名称: 州機関によるセキュリティ侵害の通知

URL: <https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2054.htm#2054.1125>

施行状況: 2009年9月1日制定、2017年9月1日・2019年9月1日改正

① 「個人情報」の定義	<p>1.個人識別情報とは、単独で又は他の情報と組み合わせで個人を識別することができる情報をいい、以下のものを含まず。</p> <ul style="list-style-type: none">A. 氏名、社会保障番号、生年月日、または政府発行の ID 番号B. 母親の旧姓C. 指紋、声紋、網膜または虹彩の画像を含む固有の生体データD. 固有の電子識別番号、住所又は経路コードE. 刑法第 32 条第 51 項に定義される電気通信アクセス装置 <p>2.機微な個人情報(以下「SPI」といいます。)には、個人の氏名、または、ファーストネームのイニシャルと姓の組み合わせに、以下の項目のいずれか 1 つ以上を組み合わせたものが含まれ、氏名と項目が暗号化されていない場合をいいます。</p> <ul style="list-style-type: none">A. 社会保障番号B. 運転免許証番号または政府発行の ID 番号C. 口座番号、クレジットカード番号、デビットカード番号と、個人の金融口座へのアクセスを許可するために必要なセキュリティコード、アクセスコード、パスワードの組み合わせ <p>SPI には、個人を特定する、以下に関連する情報も含まれます。</p> <ul style="list-style-type: none">D. 個人の身体的または精神的な健康状態E. 個人に対するヘルスケアの提供F. 個人への医療提供のための支払い <p>なお、SPI には、連邦政府または州もしくは地方政府から合法的に公開されている情報は含まれません。</p>
② 法律の適用範囲	TDBA は、テキサス州でビジネスを行い、SPI を含むコンピュータデータを所有またはライセンス供与しているすべての民間企業に適用されます。ただし、金融機関は TDBA の対象ではありません。
③ 地理的範囲	TDBA は、テキサス州に所在するデータ対象者に適用さ

	れますが、テキサス州外で事業を行う企業もこの法律に従わなければなりません。
--	---------------------------------------

- ii. 上記の法について特に言及すべき事項がございましたらその概要をご教示下さい。

個人情報の窃盗 個人識別情報を、本人の同意または有効な同意なしに、他人の名義で商品、サービス、保険、信用供与、またはその他の有価物を取得する目的で、取得、保有、移転、または利用してはなりません。

個人情報の保護 事業者は、事業者が収集または保有する SPI の違法な利用または開示から保護するために、適切な是正措置を取ることを含む合理的な手順を実施し、維持するものとします。

事業者は、事業者の保有または管理下にある SPI を含む顧客記録のうち、事業者が保持すべきでないものを、次の方法で破棄するか、破棄するよう手配しなければなりません。

- (1) シュレッダーで処理する。
- (2) 消去する。
- (3) その他の手段により、記録中の SPI を読み取り不能または解読不能な状態に変更すること。

通知義務 SPI のデータ侵害が発生した場合、事業者および州機関は、影響を受ける個人に通知する必要があります。さらに、テキサス州民 250 人以上に対するセキュリティ侵害の通知を行う必要がある企業や州機関は、60 日以内に司法長官にもその侵害を通知しなければなりません。2021 年 9 月 1 日時点で、当該事業者が別のデータ侵害を経験しない限り、司法長官は、TDBA の下で事業者から受け取った通知のリストを 1 年間公表します。

さらに、TGDBA では、SPI の侵害、侵害の疑い、または不正な開示の発見後 48 時間以内に、州機関は (a) 最高情報セキュリティ責任者を含むその部署、または (b) 侵害、侵害の疑い、または不正な開示が選挙データに関わる場合は州務長官、に通知しなければなりません。

さらに、TGDBA では、SPI の侵害の根絶、終結、回復の日から 10 日以内に、州機関は、最高情報セキュリティ責任者を含む部門または事案の詳細を通知しなければならず、その通知に事案の原因の分析を含めなければなりません。

III. OECD プライバシーガイドライン

- i. OECD プライバシーガイドラインの各原則を体現した法の規定があればその概要をご教示下さい。

<https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>

- (a) 収集制限の原則

該当する規定はありません。

- (b) データ内容の原則

この原則について明記した規定はありませんが、企業または公共機関が SPI の安全性、機密性、または完全性を損なうコンピュータ化されたデータの不正取得を経験した場合、当該企業は影響を受ける個人、およびテキサス州司法長官(該当する場合)に通知することが義務付けられています。

- (c) 目的明確化の原則

該当する規定はありません。

- (d) 利用制限の原則

該当する規定はありません。

- (e) 安全保護の原則

この原則について明記した規定はありませんが、企業または公共機関が SPI の安全性、機密性、または完全性を損なうコンピュータ化されたデータの不正取得を経験した場合、当該企業は影響を受ける個人、およびテキサス州司法長官(該当する場合)に通知することが義務付けられています。

- (f) 公開の原則

該当する規定はありません。

- (g) 個人参加の原則

TDBA に基づく私的な訴えの権利はありませんが、TDBA に基づく違反はテキサス欺

臆的取引慣行法の違反となる可能性もあり、私的な訴えの原因を生じさせる可能性があります。

(h) 責任の原則

テキサス州司法長官は、いかなる違反に対しても、1回の違反につき2,000ドル以上50,000ドル以下の民事罰を課すことができます。さらに、通知義務の不履行に対する民事罰は、通知義務を負う者1人当たり、1日につき100ドルまで、1回の違反につき25万ドルを超えない範囲で引き上げられます。

また、司法長官は、250人以上のテキサス州民のデータ侵害に関連する情報を1年間、公共のウェブサイトで公開します。

- ii. OECD プライバシーガイドラインの各原則が適用されない分野があればその概要を教えてください。

IV. ガバメントアクセスとデータローカライゼーション

あなたの国において、包括的なガバメントアクセスやデータローカライゼーションのような、個人データの主体の権利に影響を及ぼすような仕組みはございますか。ある場合は、その内容をご教示下さい。

テキサス州法にはデータのローカライズと政府アクセスに関する規則はありませんが、米国企業は理論上、外国情報監視法第702条（「FISA 702」）、および行政命令12333（「EO 12333」。FISA 702と合わせて「米国政府監視法」といいます。）に基づいてFBIが発行する国家保障書簡の要請といった米国政府監視法の対象となる可能性があります。米国政府の責任と政策により、情報収集は対外情報目的に必要なものに限定され、商業的利益を含むその他の目的での情報収集は明示的に禁止されています。

FISA 702の違反が発生した場合、日本国民および日本居住者を含む個人は、いくつかの米国法令に基づき、当該違反の救済を求めることができます。FISAに基づく違法な監視の対象となった個人は、違反を犯した個人に対して損害賠償、懲罰的損害賠償、弁護士報酬を請求することができます。さらに、電子通信プライバシー法（「ECPA」）に基づき、FISA第702条の違反について、

政府に対し、補償的損害賠償と弁護士報酬を求める別の私的権利規定が存在します。また、個人は、行政手続法(5 U.S.C. § 702(2018年))により、「特定の政府行為のために法的過誤を被る」個人が、その行為を差し止める裁判所の命令を求めることもでき、違法な FISA に基づく監視に異議を唱えることができます。したがって、上記のように、日本国民または居住者は、FISA 第 702 条の違反に対する救済を求めることができます。

V. データ保護機関

データ保護機関がある場合は、名称と住所をご教示下さい。

なし