ブラジル個人情報保護法の施行

柏　健 吾（TMI 総合法律事務所）

2018 年 8 月 14 日に成立したブラジルの個人情報保護法（Lei Geral de Proteção de Dados Pessoais。2018 年法 13709 号。以下「LGPD」という。）が、2020 年 9 月 18 日に施行された。LGPD 施行前は、個人情報の目的外利用や漏洩については、当該個人（LGPD では「titular」（日本語で保有者）という用語が使用されているが、EU 一般データ保護規則（以下「GDPR」という）の文脈で一般的に使用されている「データ主体」という用語を本稿では用いることとする。）は、消費者保護法違反などを理由に損害賠償請求をしてきた。LGPD は、個人情報の取扱いを包括的に規定したブラジルでの初めての法律である。本稿では、LGPD の概要とともに、LGPD の現状を踏まえて企業として対応すべきことを解説する。

Ⅰ　LGPD 成立から施行までの経緯～施行日をめぐる混乱～

LGPD は、2018 年 8 月 14 日に成立し、当初の施行日は法律公布後 18 か月後であった。ところが、監督官庁の設置の遅れや企業の対応の遅れ等を考慮し、2019 年法 13853 号により、施行日は法律公布後 24 か月後に延期された。

その後、2020 年に入り、再度施行日の延期が国会で議論され、その中で、LGPD の行政上の制裁（警告や制裁金など）に関する条文については 2021 年 8 月 1 日から適用されることが決定された。その他の規定についても 2021 年 5 月に施行される内容で議論されていたが、最終的には、2021 年 5 月施行を定めた暫定措置令が 2020 年 9 月 18 日に却下され、同日から LGPD が施行されることになった。

Ⅱ　LGPD の概要

1.　主要な用語の定義

LGPD で用いられる主要な用語の定義は以下のとおりである（LGPD5 条）。

個人データ	個人が特定される又は特定され得る情報
センシティブデータ	（個人データのうち）人種、民族、信仰、政治的意見、労働組合又は宗教・哲学・政治団体の加入の有無、健康、性向、遺伝、生体等に関する情報
データ主体	個人データから特定される自然人
管理者	個人データの取扱いに関して意思決定を行う者

処理者	管理者のために個人データの処理を行う者
処理エージェント	管理者及び処理者

LGPD の「個人データ」の定義は上述のとおり非常に簡潔なもので、GDPR のように具体的な例示がない。そのため、あらゆる情報について、個別に個人が特定され得るか否かを判断することになる。個人データへの該当性がよく議論されるクッキーも個別に判断する必要がある。

2. 監督機関

LGPD の監督機関は Autoridade Nacional de Proteção de Dados と呼ばれる機関（以下「ANPD」という。）である。LGPD の多くの条文において、その適用要件やルールの詳細を ANPD が別途決定すると規定している。もっとも、本項執筆時点では、具体的なガイドライン等はまだ公表されていない。

3. LGPD の適用対象行為

ブラジル国内で個人データを処理する場合だけではなく、ブラジル国内向けに提供する商品又はサービスに関連して個人データを処理する場合やブラジル国内在住者の個人データを処理する場合にも適用される（LGPD3 条）。そのため、たとえば、ブラジル国内に拠点がない会社であっても、ブラジル国内向けにサービス（スマートフォンのアプリなど）を提供する場合には、LGPD の適用を受けることになる。なお、LGPD は、GDPR と異なり、国外適用の場合に、ブラジル国内に代理人を置くことを明文では規定していない。この点については、ANPD のガイドライン等で今後明らかになる可能性もあるが、LGPD の条文上は、国外の者も「管理者」となるため、後述する DPO を設置する義務を負うことになる。

4. 個人データの処理の正当化根拠

個人データの処理は、法律に定められた要件を満たす場合にのみ許される（LGPD7 条）。そのうち、一般的な企業にとって利用頻度が高いのは、①データ主体の同意、②法律上の義務の履行、③契約上の義務の履行又は契約の準備行為及び④正当な利益である。

データ主体から同意を取得する際には、他の条項と明確に区別される形で同意を取得する必要があり、また、個人データを処理する個別の目的と関連付けられる形での同意である必要がある（LGPD 5 条 12 号、8 条）。つまり、単に個人データの処理に同意するという一般的な同意では足りない。

「正当な利益」は、管理者の活動の「promotion」のためにも利用できると規定されているため（LGPD10 条 1 号）、GDPR における「正当な利益」よりも柔軟な利用が許容される可能性がある。

5. データ主体への情報提供

データ主体に対しては、①処理の目的、②処理の態様・期間、③管理者の情報、④管理者の連

絡先、⑤個人データの共有に関する情報とその目的、⑥処理を実施するエージェントの責任及び⑦データ主体の権利を、明確かつ分かりやすい方法で提供する必要がある（LGPD9 条）。

6. データ主体の権利

データ主体は、①個人データの処理の有無の確認、②個人データへのアクセス、③個人データの訂正、④不必要・過剰な個人データ又は LGPD に違反する処理が行われている個人データの匿名化・利用停止・削除、⑤データポータビリティ、⑥同意に基づき処理されている個人データの削除（一定の例外あり）、⑦個人データの共有相手の情報の取得、⑧同意の拒否をできるか否か及び拒否した場合の効果の情報の取得、⑨同意の撤回、⑩ANPD において自己の個人データに関して管理者に対する請願を行うこと、⑪同意以外の根拠に基づく個人データの処理が LGPD に違反している場合の異議申立、⑫自己の利益に影響する自動的なデータ処理に基づく決定のレビューの要請などの権利を有する（LGPD18 条、20 条）。なお、管理者は、データ主体から個人データの有無の確認を求められたら、直ちに簡易な方法によって、又は、データ主体による要請から 15 日以内にデータの情報源や処理目的を通知しなければならない（LGPD19 条）。

7. 管理者・処理者の義務

管理者及び処理者は、個人データの取扱いを記録し（LGPD37 条）、個人データ保護のための適切な措置を講じる（LGPD46 条）。管理者は、データプロテクションオフィサー（LGPD では「encarregado」（日本語で責任者）と規定されている。以下「DPO」という。）の選任（LGPD41 条）、ANPD の要請に基づきインパクトレポートと呼ばれる個人データの処理内容等が記載されたレポートの作成（LGPD38 条）、事故（情報漏えい等）発生時の ANPD やデータ主体への報告等の義務を負う（LGPD48 条）。

8. 国外移転

個人データのブラジル国外への移転は法定の要件を満たした場合にのみ許される（LGPD33 条）。具体的には、ANPD が個人データの保護が十分と認定した国に移転する場合、管理者が個人データの保護に十分な対策を講じた場合（標準契約条項の締結、拘束的企業準則など）、データ主体からの同意がある場合などである。なお、本稿執筆時点で、いずれの国も個人データの保護が十分な国として認定されていない。

9. 罰則

LGPD に違反した場合、行政上の処分として、警告、違反の公表、個人データの停止又は削除、制裁金（グループ会社全体のブラジルでの売上の 2%以内、上限は 5000 万レアル）等を課せられる（LGPD52 条）。なお、かかる罰則のほか、民事上の損害賠償責任も負う（LGPD42 条）。

10. 2019 年法 13853 号による法改正

2019 年法 13853 号は、施行日の変更だけではなく、内容的な改正もいくつか行っている。主なものは、以下のとおりである。

5 条 8 号	DPO は自然人がなるという規定が削除された（法人も DPO になれる）。また、処理者も DPO を選任することが追記された
7 条 7 項	一定の条件のもと、公開されている情報を別の目的で使用できるようになった
11 条 4 項	経済的利益を得るためのセンシティブデータの管理者間の共有に関して、一定の条件のもと、医療サービス、調剤支援及びヘルスケアの提供においては例外的に認められることになった
11 条 5 項	保険会社が契約又は受益者の加入・排除に関するリスクを選別するために健康情報を使用することが禁止されることになった
52 条 7 項	情報漏洩等が発生した場合に、データ主体と管理者間で和解した場合は、LGPD の行政上の制裁が課せられないことになった

III 現時点で行うべき対応

1. 義務の範囲が不明確である状況での対応方針

管理者や処理者に課せられる LGPD 上の義務について、ANPD による具体的なガイドライン等は本稿執筆時点ではまだ公表されていない。そのため、どのように対応すべきか判断に迷う企業も多い。このような状況においては、その時点で適切であろうと考えられる対応をまずは行うこととなる。そして、適切であろう対応は、保有・処理する個人データの内容によって異なり得る。たとえば、センシティブデータを取り扱うような場合は、情報漏洩時の影響が大きいため、非常に厳格な対応をすべきであろう。

2. 具体的な対応

LGPD の全体像は GDPR と非常に似ている。そのため、GDPR への対応をすでに行っている企業は、それと同様の対応を LGPD に関しても行えば基本的な対応としては十分である。

一方、ブラジルにおける事業内容や保有する個人データの内容から GDPR ほどの対応は不要なケースもあるであろう。もっとも、そのような企業であっても、以下の作業は最低限行っておくべきである。

(1) データマッピング

自社が保有する個人データの内容や取得経緯を確認し、その処理について法的根拠があるかを確認する。仮に法的根拠がないのであれば処理を停止する。データ主体からの同意取得で解決できる場合には同意を取得する（たとえば、従業員情報の日本本社への提供に関して従業員から同意を取得する）。

(2) プライバシーポリシーの作成

上記Ⅱ、5 で記載したとおり、個人データの処理のためには、データ主体に対して、処理の目的等の情報を提供する必要がある。実務的には、これらを規定したプライバシーポリ

シーを作成し、自社ウェブサイトにおいて掲載する形で情報提供することが一般的である。また、データ主体から個人データの処理に関する同意を取得する際には、プライバシーポリシーに同意させるプロセスを作る必要がある。

(3) 情報漏洩等発生時の対応プロセスの明確化

情報漏洩等の事故は、管理者がもっとも責任を問われる事象であるため、そのような事態が生じた場合の社内対応プロセス（特に誰に情報を集約させるか）を明確にしておくべきである。