

コロンビアにおけるデータ保護規則

(2021年3月)

日本貿易振興機構(ジェトロ)

ボゴタ事務所

ビジネス展開支援課

報告書の利用についての注意・免責事項

本報告書は、日本貿易振興機構（ジェトロ）ボゴタ事務所が現地法律事務所 Lloreda Camacho & Co.に作成委託し、2021年3月に入手した情報に基づくものであり、その後の法律改正などによって変わる場合があります。掲載した情報・コメントは作成委託先の判断によるものですが、一般的な情報・解釈がこのとおりであることを保証するものではありません。また、本報告書はあくまでも参考情報の提供を目的としており、法的助言を構成するものではなく、法的助言として依拠すべきものではありません。本報告書にてご提供する情報に基づいて行為をされる場合には、必ず個別の事案に沿った具体的な法的助言を別途お求め下さい。

ジェトロおよび Lloreda Camacho & Co.は、本報告書の記載内容に関して生じた直接的、間接的、派生的、特別の、付随的、あるいは懲罰的損害および利益の喪失については、それが契約、不法行為、無過失責任、あるいはその他の原因に基づき生じたか否かにかかわらず、一切の責任を負いません。これは、たとえジェトロおよび Lloreda Camacho & Co.に係る損害の可能性を知らされていても同様とします。

本報告書に係る問い合わせ先：

日本貿易振興機構（ジェトロ）
ビジネス展開・人材支援部 ビジネス展開支援課
E-mail：BDA@jetro.go.jp

ジェトロ・ボゴタ事務所
E-mail：CBO@jetro.go.jp

JETRO

目 次

1. はじめに	1
2. 重要事項	1
3. 実証責任	2
4. RNBD に個人データを取り扱うデータベースを登録する義務	3
5. 個人データ侵害に関する犯罪	4
6. 罰則	4
7. 最近の進展	4

コロンビアにおけるデータ保護規則

1. はじめに

コロンビアでは、データ保護に関する全般的な規則は 2012 年から施行された。2012 年法律 1581 号（データ保護総合法：LGPD）が発行される前に、国政府は財務データの保護に適用される特定の規則を定めていた。また、1991 年憲法には、基本的権利としてデータ保護が含まれているが、これらの規定は、個人データとプライバシーを総合的に保護するためには効果的ではなかった。

LGPD の発行以来、その主な目標は、データ所有者（その人たちについての情報が取り扱われる）の権利を保護し、データを取り扱うすべての企業が一般的な要件に準拠することを保証することである。それ故、企業は、規則を遵守できるよう、個人データの取り扱いについて明確に定めていなければならない。

2. 重要事項

個人データの保護については、LGPD とその施行規則、および 2015 年商工監督局（SIC）通達 002 号、また SIC 総合通達第 V（5）章に定められている。この規則には、2012 年から施行されており、データの収集、保管、使用、その他データに実施するあらゆる種類の操作（「取り扱い」）について最低要件が定められている。

個人データとは、データの所有者とみなされる単数または複数の個人（「所有者」）に関連する、あるいは結びつくあらゆる情報を意味する。

データ取り扱いは、個人または組織（取扱責任者）が直接、または責任者に指定された第三者（取扱担当者）が行うことができる。

LGPD は、以下のデータベースに保管されている個人データには適用されない。

- a. 個人、あるいは家庭のデータベース
- b. 国家安全保障および防衛、およびマネーロンダリングおよびテロ資金供与の防止、検出、監視、および制御に関するデータベース
- c. 諜報および防諜に関するデータベース
- d. ジャーナリズム情報
- e. 財務情報および信用情報（2008 年法律 1266 号）
- f. 国勢調査（1993 年法律 79 号）

個人データ取り扱いの法的な正当性は、所有者から与えられた同意に基づく。それ故、所有者の明確な同意なしに行われるあらゆる個人データの取り扱いは、同意が必要とされない場合以外、違法とみなされる。

つまり、データ保護法第 10 条に記載された場合のみ、個人データ取り扱いについての同意が必要ないとされ、それらは次のとおりである。

- i. 公的機関あるいは行政機関の通常の業務上必要な情報、あるいは司法命令により必要な情報。
- ii. 公開データ
- iii. 医療または健康上の緊急事態
- iv. 歴史的、化学的、統計的な目的のために法律により許可されているデータ取り扱い
- v. 戸籍登記に関する情報

重要な概念は、センシティブデータについてである。センシティブデータとは、政治や宗教についての考え、生体認証情報、医療または臨床情報などを指す。センシティブデータの取り扱いには、通常よりも具体的な同意を得る必要がある。また、この種のデータの取り扱いについては、所有者に対して、所有者がセンシティブデータを提供することは義務ではないことを通知しなければならない。

取扱責任者は、様々な義務を順守しなければならない。その中でも重要なものは次のとおりである。

- i. 会社によるデータ取り扱いに関するすべての社内要件を定めたポリシーを導入すること。プライバシーポリシーには、少なくとも以下を含める必要がある。
 - (a) 取扱責任者の氏名または会社名、居住地、住所、電子メール、電話番号
 - (b) データ取り扱いの目的
 - (c) 所有者の権利
 - (d) データを知り、更新し、修正し、削除し、同意を取り消す権利を行使するために、当事者が申請を提出する宛先となる、申請、問い合わせ、クレームの対応者または責任者
 - (e) 権利を行使する方法について所有者に通知する手順
 - (f) プライバシーポリシーの発効日とデータベースの期間
- ii. 個人データの取り扱いには、常に事前に明確な同意を得る必要がある。同意を取得するには、収集されるデータの種類やデータ取り扱いの目的などを知らせなければならない。同意は、口頭、書面、または当事者の明確な行為を通じて得ることができ、いずれの場合でも、当事者がいつでも検証あるいはアクセスできるよう備えなければならない。
- iii. 情報の用途は、所有者により与えられた同意に記載された目的だけに限られる。
- iv. その義務がある場合、取扱責任者は、国家データベース登記（RNBD）にデータベースの登録を行わなければならない。

3. 実証責任

2013年規制令1377号では、取扱責任者がLGPDの順守を保証するための義務がある、実証責任（説明責任）について定められている。

上記規則では、取扱責任者は、法律を遵守して、責任をもって行動したことを実証

できなければならない、と定めている。実証責任プログラムを導入するためには、企業は次のことを考慮しなければならない。

- i. データプライバシーに関する明確で効果的な社内ポリシーを有していること。
- ii. コンプライアンスメカニズムを導入すること。
- iii. プライバシーオフィサー（DPO）など、データ保護について監督する者を一人あるいは複数任命すること。
- iv. データの安全と機密性を保証する必要性について、人々を教育し、啓発するための手順を導入すること。
- v. リスクを評価し、リスクを減少する能力をもつこと。
- vi. データプライバシーと関連する事項の実施を恒常的に検証すること。
- vii. 上記の安全に関する措置、および当事者の権利行使のためのメカニズムを導入すること。

4. RNBD に個人データを取り扱うデータベースを登録する義務

2021 年の総資産が 36 億 3 千 80 万ペソを超える取扱責任者はすべて、そのデータベースを RNBD に登録する必要がある。当該登録には、取扱責任者が会社のデータベースについての全般的な情報を登録することが必要であり、その中には次のものが含まれる。

- i. 取扱責任者および取扱担当者の連絡先情報。
- ii. データ取り扱いの目的。
- iii. 具体的なデータベースに登録されたデータの種類。
- iv. 登録されている所有者数。
- v. 所有者の権利行使のためのメカニズム。
- vi. 個人データの源（どのようにデータを取得したか明らかにすること）。
- vii. データの送信や転送（国際的あるいは国内）。
- viii. それぞれのデータベースに適用される安全措置。

新しいデータベースは、作成から 2 カ月以内に登録しなければならない。登録は、少なくとも次の場合には更新しなければならない。

- i. 毎年最初の 3 カ月、1 月 2 日～3 月 31 日の間。このときには、全体的な更新を行う必要があり、登録されている当事者数などのデータを更新しなければならない。
- ii. 当事者からのクレーム、問合せ、要求は、毎年 2 月と 8 月の最初の営業日 15 日間に登録しなければならない。2021 年の場合には、遅くとも 2 月 19 日と 8 月 23 日までに行う必要がある。この場合、8 月の報告には、その年の上半期のクレーム、問合せ、要求を含める必要があり、下半期に受け付けられたクレーム、問合せ、要求などは 2 月に登録されることになる。
- iii. データベースの大幅な変更（例えば、データ転送、目的の変更、新しいデータプロセッサなど）は、変更があった翌月の最初の営業日 10 日間以内に登録しなければならない。
- iv. セキュリティインシデントについては、インシデントが把握された日から営業日

15 日間以内に通知されなければならない。

登録は SIC のウェブページを通じて行うが、比較的容易である。

5. 個人データ侵害に関する犯罪

コロンビア刑法には、「情報やデータの保護」と関連する犯罪が含まれている。269F 条では、「個人データの侵害」について次のように定めている。そのために許可されていない者が、自分の利益あるいは第三者の利益のために、ファイル、アーカイブ、データベース、または同様の媒体に含まれる個人データ、個人コードを取得、編集、除去、提供、販売、交換、送信、購入、傍受、開示、変更、または使用する者は、48 カ月から 96 カ月の懲役、および、現行の法定最低賃金 100 カ月～1,000 カ月相当の罰金が科せられる。

それ故、何らかの情報の侵害や漏洩が発生した場合、誰でもこの条項に基づき告発を提出することができる。刑法の違反とは別に、SIC は違反または漏洩についての調査を開始することができる。

6. 罰則

SIC は、LGPD の規定に違反した者に対し、行政調査を開始し、最大で法定最低賃金 2,000 カ月相当（2021 年は 18 億 1 千 705 万 2,000 ペソ）の罰金を科すことができる。また、個人データの一般的な規則に違反した者の専門的あるいは商業的活動の一時的または恒久的な閉鎖を含む罰則を科すことができる。罰則は、会社、取締役やマネージャーにも個別に適用できる。

7. 最近の進展

2020 年 12 月に、SIC は、個人データの取扱責任者と担当者を対象とした 2 つの新しいガイダンスを発行した。公開されたガイダンスは、実証責任ガイドに加えて、マーケティングおよび広告目的のデータ取り扱いなどについて言及している。これらの新しいガイダンスは、コロンビアの個人データ保護制度に対する不正を防止するために便利なツールやアドバイスを含んでいる。取り上げられているテーマは次のとおりである。

- i. 個人データとしての写真の取り扱い。
- ii. 個人データ取り扱いにおけるセキュリティインシデントの管理。

これに関し、これらのガイダンスは、その活動実施において個人データ取り扱いを行う者の自主規制を強化するための全般的な推奨事項を提供するためのものであることを記載することが重要だろう。

同様に、これらのガイダンスは、写真の取り扱いやセキュリティインシデントの管理に関し、すべての重要事項を網羅しているわけではないことを特筆する。それ故、それぞれのケースについての具体的な要件を確認するには、すべての適用可能な規則を照会することが重要である。

i. 個人データとしての写真の取り扱いに関するガイダンス

SIC が指摘するように、写真を使用する場合、これらに個人データが含まれていることが無視されることがよくある。一般に、写真に含まれる 1 人または複数の人について、個人の身元を確認することが可能な生体情報を有する写真である場合、写真が個人データを含んでいることになる。

その意味で、SIC は、写真を個人データとして扱うことに関連する最も重要な義務のいくつかをまとめた。それらは次のとおりである。

- (a) 写真を撮り、それらを使用するには、事前の明確な許可を得ること。また、写真を撮り使用することを知らせること。
- (b) 第三者から提供された写真の場合、その出自が合法的であることを確認すること。
- (c) 18 歳未満の未成年者の写真を撮り、使用するには、これらのデータの特別かつセンシティブな性質を考慮して、そのための規則を念頭に置くこと。
- (d) 提供された写真が使用される具体的な目的をデータ所有者に知らせること。
- (e) 不正な方法で写真を入手することは控え、パブリックアクセスの写真を自由に使用してよいと思わないこと。
- (f) その名前や責任において写真を撮るために契約した第三者に、データ保護の規則遵守を要求すること。

最後に、写真には個人データが含まれているため、この問題に適用される規則によって保護されている上に、著作権、不公正な競争、肖像権などの様々な法的観点からも保護されていることを明らかにすることが重要だろう。上記のガイダンスでは、この規定が個人的または家庭的な領域での写真の使用や、ジャーナリズムおよび編集目的での写真の使用を制限するものではないと述べている。

ii. 個人データ取り扱いにおけるセキュリティインシデント管理のためのガイダンス

SIC は、データ取扱責任者および担当者によって管理される個人データを含むデータベースに影響を与えるセキュリティインシデントの発生と報告に正しく対処するための一連の実用的なアドバイスを公開した。

2012 年法律 1581 号に従い、責任者または担当者が行う個人データの取り扱いは、当該情報の安全性と機密性を保証するために必要な技術的、人的、および管理上の措置を講じて行われなければならない。

そのため、組織は、前述のセキュリティ対策が機能しない場合に発生する可能性のある影響またはリスクを軽減する備えがなければならない。従って、SIC が発行したガイダンスは、次のような措置の実施に関する手引きを提供している。

- (a) データ取扱担当者に、発生しうるセキュリティインシデントについて通知するよう要求すること。
- (b) セキュリティインシデントについて、しかるべく記録すること。
- (c) セキュリティインシデントの管理における対応プロトコルを含む、個人デー

タ管理の総合的なプログラムを策定すること。

- (d) セキュリティインシデントに対処するために必要なステップを導入すること。

このガイダンスでは、個人データの取り扱いを伴うすべての活動を確立するための基本的な要件として、組織内の個人データの所有者の信頼を高め、維持する必要性も強調している。

最後に、両方のガイドは、データ取り扱いにおける実証責任の原則を適用することが必要であることを繰り返している。それ故、この原則に関して SIC によって発行されたガイダンスに記載されていることを考慮する必要がある。