グローバル個人データ保護方針

分類	公開
文書バージョン	2.0
発行日	2026 年 2 月 26 日

目次

1. はじめに 3
2. 目的 3
3. 定義 3
4. 個人データ処理の基本原則 4
5. 処理活動の記録 4
6. 合法性と妥当性 5
6.1 個人データ処理の法的根拠 5
6.2 プライバシー評価 5
6.2.1 プライバシー・バイ・デザイン評価 5
6.2.2 データ保護影響評価（DPIA） 5
6.2.3 データ移転影響評価（DTIA） 5
6.2.4 合法的利益影響評価（LIIA） 6
6.2.5 機密データ及び特別区分データの取り扱い基準 6
6.2.6 バルク・データ・ルール 6
6.3 契約上の保護 6
6.3.1 グループ内データ移転協定（IGDTA） 6
6.3.2 データ処理協定（DPA） 6
6.3.3 一般プライバシー規定 7
7. 精度と保持 7
7.1 記録管理 7
7.2 個人データの保管とバックアップ 7
7.3 個人データの消去又は破壊 7
8. 機密性と完全性 8
8.1 情報セキュリティ 8
8.2 テスト 8
8.3 個人情報インシデントの報告 8
8.4 個人情報インシデントへの対応 9
9. 透明性 9
9.1 プライバシー通知 9
9.2 トレーニング 10
9.3 データ主体の権利 10
9.4 監督当局 11
9.5 データ保護責任者 11
10. 順守 11
11. 例外 11
12. 所有権と改訂履歴 11

1. はじめに

Entrust Corporation 及びその子会社（総称して「Entrust（エントラスト）」又は「当社」）は、データ管理者としての役割の下、当社の従業員及び当社の販売パートナー、サプライヤ、顧客の取引先担当者に関する個人データを処理します。また、Entrust はデータ処理者としての役割において、当社の顧客及び従業員、エンドユーザに関する個人データも処理します。Entrust が個人データを処理する場合、当社は法律上及び契約上の義務を順守し、完全な透明性をもって行います。

2. 目的

本ポリシーは、Entrust が関連する法律及び契約上の義務、ならびに認証及び監査要件を確実に遵守するために制定した、当社のグローバルデータプライバシープログラムの要件及び要素を規定するものです。本ポリシーは、Entrust が世界で行うすべての個人データ処理に適用されます。

3. 定義

「データ管理者」とは、個人データ処理の目的及び手段を決定する主体を意味し、ISO 27701 の「PII 管理者」と同じ意味です。

「データ処理者」とは、データ管理者に代わって個人データを処理する主体を意味し、ISO 27701 における「PII 処理者」と同じ意味です。

「データ保護影響評価」は、データ管理者又はデータ処理者が、処理がデータ主体の権利及び自由に対して高いリスクをもたらす可能性がある場合に、プライバシーリスクを評価する文書化された分析を指します。

「データ保護法」は、Entrust に適用されるすべての個人データ保護及びプライバシーに関する法律及び規制を指しており、これには、EU 一般データ保護規則（GDPR）、英国一般データ保護規則（UK GDPR）、英国データ保護法（DPA 2018）、スイス連邦データ保護法（2023 年 9 月 1 日施行）（FADP）、カナダ個人情報保護及び電子文書法（PIPEDA）、日本の個人情報保護法（APPI）、中国の個人情報保護法（PIPL）、及び米国各州のプライバシー法が含まれますが、これらに限定されず、いずれの場合でも、修正、廃止、又は置換される場合があります。

「データ主体」とは、個人データが関係する、特定又は識別可能な個人又は世帯を意味し、ISO 27701 での「PII 主体」と同じ意味です。

「データ移転影響評価」は、欧州経済領域（EEA）又は英国内から、欧州委員会又は情報コミッショナー事務局による適切性認定を受けていない EEA/英国外の国への個人データの移転が持つ影響及びセキュリティへの影響に関する、データ管理者又はデータ処理者が文書化した分析を指します。

「正当な利益影響評価」は、正当な利益を個人データ処理の法的根拠として使用できるかどうかについて、データ管理者又はデータ処理者が文書化した分析を指します。この評価には、個人データ処理が正当な利益の追求であるかどうか、その追求のために必要であるかどうか、データ主体の利益が正当な利益よりも優先されるかどうかを分析する三重構成のテストが含まれます。

「個人データ」又は「**PII**」は、「個人を特定できる情報」、「個人情報」、又はデータ保護法で定義されているこれらの用語と同等の用語に付与されている意味を有します。

「個人データインシデント」は、「セキュリティインシデント」、「セキュリティ侵害」、「個人データ侵害」、又はデータ保護法で定義されているこれらの用語と同等の用語に付された意味を有し、個人データが不正な方法で、不正な者によってアクセス、開示、改ざん、紛失、破壊、又は使用されたことを Entrust が認識した状況を含みます。

「処理」とは、収集、記録、組織構造化、保管、適応又は変更、検索、相談、使用、送信による開示、普及又はその他の提供、整列又は組み合わせ、制限、消去、又は破棄など、自動的な手段によるものであるか否かを問わず、個人データに対して行われるあらゆる操作又は一連の操作を意味します。処理には、個人データの第三者への譲渡または開示も含まれます。

「機密性の高い個人データ」は、個人データのサブセットであり、紛失した、危殆化された、アクセスされた、又は不適切に開示された場合、データ主体に危害、困惑、不便、又は不公正をもたらす可能性があり、したがって高度な保護の対象となるデータ主体に関する情報を指します。

「特別区分データ」は、個人データのサブセットであり、個人の人種や民族的出身、政治的意見、宗教的又は哲学的信条、労働組合への加盟に関する情報、及び遺伝データ、自然人を一意に識別するための生体認証データ、健康に関するデータ、自然人の性生活又は性的指向に関するデータの処理を指します。

4. 個人データ処理の基本原則

Entrust は、データ管理者として個人データを処理する際、以下の基本原則を厳守します。

- 合法性と妥当性：当社は、個人データが合法的な目的のために収集され、その目的に適切かつ必要なものに限定されることを保証します。
- 精度と保持：当社は、システムを最新の状態に保ち、不正確な個人データを更新するための仕組みを提供し、処理の合法的な目的を果たすのに必要な期間を超えて個人データを保持しません。
- 機密性と完全性：当社は、個人データが処理中も安全かつ保護されていることを保証しますが、個人データのインシデントが発生した場合には、必要に応じて適時に通知を行うなど、迅速かつ適切に対応します。
- 公平性と透明性：当社は、個人データを処理する際、データ対象者に適切に通知します。当社は、なぜその情報が必要なのか、どのように利用するのか、どのように取り扱い保護するのかを明確にします。当社は、データ主体が適用法の下で個人データに関して有する権利を行使するための仕組みを提供します。

Entrust の全社員は、個人データを適切に処理し、保護する責任があり、これを怠ると、Entrust に対する顧客の信頼が損なわれるだけでなく、当社に多額の罰金や罰則が科される可能性があることを理解しています。

5. 処理活動の記録

適用されるデータ保護法を確実に遵守し、透明性と説明責任への当社の責務を支持するため、Entrust は GDPR 第 30 条及びその他の関連プライバシー規制に従って処理活動の記録（RoPA）を維持します。RoPA には、Entrust の「Data Classification & Handling Standard（データ分類・取扱基準）」に従って分類された個人データに関わるすべての処理活動が含まれます。

6. 合法性と妥当性

6.1 個人データ処理の法的根拠

データ管理者として行動する場合、当社は法的に許可された場合にのみ個人データを処理します。Entrust は、主に以下の法的根拠に基づき処理します。

- 契約の履行、
- 法執行機関からの合法的な要請を含むがこれに限定されない、法的義務の順守、
- 正当な利益（ただし、かかる利益がデータ主体の利益又は基本的権利及び自由によって無効になる場合を除く）、及び
- 同意。

同意が処理の法的根拠となる場合、Entrust は、同意が自由に与えられ、具体的で、十分な情報に基づき、データ主体の希望を明確に示すものであることを保証します。データ主体は、理由の如何を問わず、いつでも同意を撤回する権利を有します。

6.2 プライバシー評価

6.2.1 プライバシー・バイ・デザイン評価

Entrust は、新規又は大幅に変更された製品の設計・開発の一環として、また、サードパーティのソフトウェア・アプリケーションでライセンスされたものを含め、PII が処理されるベンダーのソリューションを導入する際に、個人データ処理を上記第 4 項に記載する基本原則に照らして評価します。この「プライバシー・バイ・デザイン」評価は、Entrust の開発及びベンダーの新人研修プロセスに組み込まれています。評価の完了には、Entrust のプライバシー及び情報セキュリティチームによる審査と承認が必要です。承認なしに開発を進めることはできません。

6.2.2 データ保護影響評価（DPIA）

個人データ処理が個人の権利と自由に対して高いリスクをもたらす場合、Entrust は DPIA を完了させ、データ処理の目的、当社が関連データ保護法をどのように遵守するか、データ主体に対する潜在的なリスクをどのように軽減するかを文書化し、評価します。DPIA が Entrust がデータ管理者である Processing に関連する場合、DPIA は Entrust のデータ保護責任者によって審査され、データ保護責任者は提案された処理を開始する前に承認しなければなりません。DPIA は、適用される法規制への継続的な遵守を確保するため、少なくとも年 1 回、あるいは必要に応じてそれ以上の頻度で見直し、更新するものとします。

6.2.3 データ移転影響評価（DTIA）

Entrust が、欧州経済領域（EEA）又は英国（UK）内から、欧州委員会又は英国情報コミッショナー事務局による適切性認定の恩恵を受けない EEA 又は英国外の国に個人データを転送する予定がある場合、特に受信国の法律により転送される個人データへの政府によるアクセスが認められる場合、Entrust は正式な DTIA を完了させ、転送の影響とセキュリティ上の影響を分析します。Entrust は、譲渡によってもたらされるリスクが許容できると判断した場合にのみ、譲渡を進めます。DTIA は、適用される法律および規制への継続的な遵守を確保するために、少なくとも年に 1 回、または必要に応じてより頻繁にレビューおよび更新されるものとします。

6.2.4 合法的利益影響評価（LIIA）

Entrust がデータ管理者として行動し、個人データ処理の法的根拠として正当な利益に依拠する場合、当社は正式な LIIA を完成させ、正当な利益を文書化し、評価し、処理が必要であるかどうかを判断し、データ主体の利益、権利、自由が正当な利益よりも上回る又は優先されるかどうかを評価します。Entrust は、LIIA が正当な利益よりも優先されないと結論付けた場合に限り、正当な利益に基づいて処理を進めます。

6.2.5 機密データ及び特別区分データの取り扱い基準

データ管理者としての役割において、Entrust は、様々な業務システムにおける従業員に関する機密性の高い個人データ、および一部の限定的な特別区分データを、自主的に、かつ現地法で許可された範囲内で処理します。適切な管理を施行し、適用される DPIA、Access Control Standard for Sensitive and Special Category Data（機密・特別区分データのアクセス管理基準）、およびこの機密・特別区分データを取り扱う従業員向けに許可されたプライバシー研修で概説します。

6.2.6 バルク・データ・ルール

米国市民のヒトオミックスデータ、生体認証識別子、正確な地理位置情報データ、個人の健康データ、個人の金融データ、特定の個人識別子などの機密性の高い個人データ、および搾取のリスクが高いと具体的に指定された区域（たとえば軍事施設、国家安全保障、防衛、諜報施設、連邦国家情報局職員の職場など）の正確な地理位置情報データを含む米国政府のデータは、輸出、移転、アクセスへの制限の対象となります。このようなデータは、「懸念国」に所在する個人又は団体、あるいはその個人又は団体に支配されている個人又は団体、あるいはその個人又は団体の指示によって行動する個人又は団体に提供することはできません。現在「懸念国」とされているのは、中国（香港、マカオを含む）、キューバ、イラン、北朝鮮、ロシア、ベネズエラです。

このような転送やアクセスは特定の状況下では実現される可能性がありますが、Entrust は、米国の機密性の高い個人データや米国政府のデータに関わる懸念のある国との取引には関与しないと決定しています。このようなデータは、絶対に、Entrust 又はその代理を務める者によって、懸念される国又は懸念される国に所在する個人又は団体に転送してはなりません。

6.3 契約上の保護

6.3.1 グループ内データ移転協定（IGDTA）

Entrust Corporation 及びその子会社は、個人データが Entrust グループ内で共有される場合、これが適切なデータ共有条項（GDPR が要求する管理者-処理者条項を含む）の対象となることを保証するために、グループ内データ転送協定を締結します。IGDTA はまた、EEA/UK（欧州経済地域/英国）内から欧州委員会又は情報コミッショナー事務局による適切性認定の恩恵を受けていない EEA/UK（欧州経済地域/英国）外の国への個人データの移転が含まれる場合、Entrust グループ内での個人データの共有に適切な保護措置（標準的な契約条項など）が講じられることを保証します。

6.3.2 データ処理協定（DPA）

Entrust のために、又は Entrust の代理として個人データを処理する Entrust グループ外の企業は、第三者（ベンダー、サプライヤ、チャネルパートナーなど）が関連データ保護法を遵守するための適切な技術的・組織的措置を講じていることを保証するために、Entrust とデータ処

理協定を締結する必要があります。Entrust は、データ処理者として行動する顧客に対し、標準的な顧客 DPA を通じて同等の責務を果たします。

6.3.3 一般プライバシー規定

プライバシーに関する契約上の文言は、顧客、サプライヤ、パートナーとの標準的な契約や、Entrust の標準的な秘密保持契約（NDA）にも組み込まれています。ベンダーやサプライヤとの契約には、バルク・データ・ルールを遵守する義務も含まれます。

7. 精度と保持

7.1 記録管理

グローバルな記録管理プログラムにより、処理された個人データの保管期間が正式に定義され、必要な期間だけ保管されること、また、指定された保管期間が終了した時点で個人データが消去、破壊、又は匿名化されることが保証されます。Global Records Management Policy（グローバル記録管理ポリシー）では、個人データを含む記録だけでなく、すべての記録の取り扱い要件を定めており、付属の Records Retention Schedule（記録保持スケジュール）は、当社が保持する記録の種類ごとに保持期間を定めています。

7.2 個人データの保管とバックアップ

Entrust は、当社が直接的及び間接的に管理する複数のサーバロケーションに個人データを保管し、バックアップします。IT 部門及び関連ベンダー（IT 部門以外が管理するクラウドホスト型アプリケーションの場合）には、保管及びバックアップを含め、これらのサーバにおける個人データの適切な取り扱いに関する標準的なガイダンスが提供されます。
Entrust は、商業的に非現実的である場合、保持期間終了時にバックアップメディア及びサーバーから個人データのコピーを削除しません。ただし、このように Entrust が保持する個人データは、使用中の個人データを保護するのと同じセキュリティ基準で保護され、個人データは引き続き機密保持の対象となり、適用される法律で要求される場合を除き、アクセスすることはできません。

7.3 個人データの消去又は破壊

Global Records Management Policy および Data Classification Handling Standard（情報分類取扱標準）は、あらゆる種類の記録を所定の保存期間が終了した時点での適正処理に向けた要件を定めています。特に、個人データを含む記録に関しては、以下の原則が適用されます：

- 指定された処理目的を達成するために必要な場合を除き、個人データを複写してはならず、作成した複写物には元の機密情報又は所有権に関する表示を残すものとします。
- 紙の記録は、保管する必要がなくなったらシュレッダーにかけ、安全に廃棄しなければならず、他のいかなる方法でも廃棄してはなりません。
- 電子形式の個人データは、不要になった時点で削除又は匿名化されるべきです。
- IT 部門は、関連する情報セキュリティポリシー及び基準に従って、個人データを含む電子機器（ラップトップ、デスクトップ、会社所有のモバイルデバイス、BYOD（個人所有機器の持ち込み）デバイス上の業務データなど）を破棄又は消去する責任を負います。

8. 機密性と完全性

8.1 情報セキュリティ

当社が個人データを処理する場合、個人データの安全性を確保し、不正又は違法な処理、偶発的な損失、破壊又は損傷から保護するために適切な措置を講じます。Entrust は、次のような方法でこれを実現します。

- 法律又は契約により義務付けられている場合、及び商業的に実行可能な場合には、静止時及び転送時に個人データを暗号化すること、
- 個人データの処理に使用されるシステム及びサービスの継続的な守秘性、完全性、可用性、及び回復力を、定期的にテスト又は演習される正式な事業復旧及び災害復旧計画を通じて確保すること、
- 物理的又は技術的なインシデントが発生した場合、個人データへのアクセスを適時に回復すること、
- 個人データを保護するために実施されている技術的及び組織的措置の有効性を定期的にテスト、測定、及び評価すること、
- 机や戸棚に個人データが保管されている場合は施錠すること、個々のモニター／画面は通行人から個人データが見えないようにすること、電子機器（コンピュータやタブレットなど）を放置する場合は施錠するか会社のシステムからログオフすることを義務付ける物理的セキュリティ基準の施行。

適切なセキュリティ管理を評価する際、Entrust は処理に関連するリスク、特に処理される個人データの偶発的又は違法な破壊、紛失、改ざん、不正な開示、又はアクセスのリスクを考慮します。

Entrust が第三者に個人データの処理を代行させる場合、当該第三者は Entrust からの書面による指示に基づき、契約規定（DPA など）に従って個人データを適切に取り扱い、少なくとも Entrust 自身のセキュリティ要件と同等の適切な技術的・組織的対策を実施します。このような仕組みがない限り、個人データが Entrust の外部で共有されることはありません。さまざまなセキュリティツール（DLP など）を導入し、個人データが許可なく組織外に出ないようにしています。

8.2 テスト

個人データは、事前に正式なセキュリティ例外の承認がない限り、Entrust のテスト環境で使用することはできません。すべてのテスト環境は、本番環境に適用される現行の基準及び管理を遵守しなければならず、テスト環境での使用が承認されたすべての個人データは、テストが完了した後、遅滞なく削除されなければなりません。詳しくは、セキュアソフトウェア開発ライフサイクル（S-SDLC）の概説をご覧ください。

8.3 個人情報インシデントの報告

個人データインシデントは、以下のような様々な形で起こり得ますが、これらに限定されるものではありません。

- 個人データを含むモバイルデバイス又はハード複写ファイルの紛失（公共交通機関に誤ってデバイスを置き忘れるなど）、
- 個人データを含むモバイルデバイス又はハード複写ファイルの盗難、

- 人為的ミス（例えば、従業員が誤って意図しない受信者に個人データを含む電子メールを送信したり、誤って個人データを変更又は削除したりすること）、
- サイバー攻撃（例えば、ランサムウェアやその他のマルウェアを含む見知らぬ第三者からの電子メールの添付ファイルを開くこと）、
- 無許可の使用／アクセスを許可すること（例えば、無許可の第三者が Entrust のオフィス又はシステムの安全な領域にアクセスすることを許可すること）、
- 物理的な破壊や損失（火災や洪水など）、又は
- 第三者がなりすまし（フィッシングやスミッシング攻撃など）により Entrust から情報を取得すること。

個人データインシデントは、以下の場合に発生する可能性があります。

- 有効なユーザアカウントに関する異常なログイン及び/又は過剰なシステムアクティビティ、
- 異常なリモートアクセス、
- Entrust の作業環境から可視の、又はアクセス可能な偽装無線（Wi-Fi）ネットワークの存在、
- 機器の故障、又は
- Entrust システムに接続又はインストールされたハードウェア又はソフトウェアのキーロガー。

個人データに関するインシデントが発生した可能性がある、又は発生しようとしていることに気付いた、又はそれを疑う理由がある従業員は、直ちに Entrust セキュリティオペレーションセンター（SOC@entrust.com）に連絡しなければなりません。

8.4 個人情報インシデントへの対応

個人データのインシデントが実際に発生した場合、又は発生が差し迫っている場合、Entrust は情報セキュリティによって維持されているインシデント対応及び処理手順を実施し、インシデントの影響を最小限に抑え、法律上及び/又は契約上の要求に応じて、規制当局、データ主体及び/又はその他の当事者に通知します。回答には通常、以下のことが含まれます。

- 発生した、又は発生する可能性のある損害又は危害の性質、原因、及び程度を特定するために事件を調査すること、
- インシデントの継続又は再発を阻止し、影響を受けるデータ対象者への危害を制限するために必要な措置を実施すること、
- 他の当事者（国のデータ保護当局、影響を受けるデータ主体、契約当事者など）に通知する義務があるかどうかを評価し、それらの通知を適時に行うこと、及び
- 規制当局又は影響を受ける当事者に通知する、又は通知しない決定を文書化することを含め、個人データインシデント及び対応措置に関する情報を記録すること。

9. 透明性

Entrust は、堅牢な内部及び外部ランディングページを通じて、グローバルデータプライバシープログラムに関する透明性を提供しています。

9.1 プライバシー通知

Entrust はデータ管理者及びデータ処理者の両方の役割として、個人データの処理についてデータ主体に通知します。この情報は、ウェブユーザ、求職者、従業員向けの Entrust の各種プ

ライバシー通知、及びこちらから入手可能な各製品のプライバシー通知を通じて入手できます。そのような通知は、以下の情報を提供します。

- Entrust が処理する個人データの種類、
- 処理の目的と法的根拠、
- 処理に用いられる第三者（該当する場合）、
- 処理の場所と期間、
- 個人データの国境を越える移転、
- 処理を行う期間、
- データ主体の権利、及び
- 人工知能／自動意思決定プロセスの詳細

9.2 トレーニング

Entrust は、従業員に対し、データ保護責任に関する必須トレーニングを毎年実施します。データプライバシー入門トレーニングは、入社時に実施され、その後は毎年実施されます。全社員を対象とした「データプライバシー入門」トレーニングに加え、Entrust は、機密データや特別区分データを取り扱う社員には「データプライバシー強化」トレーニングを、ソフトウェア製品やサービスの開発・設計に携わる社員には「プライバシー・バイ・デザイン」トレーニングを毎年受講することを義務付けています。Entrust は、必要に応じて、さらに機能別のプライバシーに関するトレーニングを引き続き策定し、整備します。

9.3 データ主体の権利

Entrust が個人データを処理する場合、データ主体はデータ保護法に基づき一定の権利を有します。これらの権利は法域によって異なりますが、データ主体は一般的に以下の権利を有します。

- Entrust が保有する個人データに関する情報を請求すること（当該情報のコピーを含む）、
- 不正確な個人データを訂正し、不完全な個人データを記入すること、
- 当社が正当な利益を追求するために個人データを処理することに反対する場合。当社の正当な利益がデータ対象者の利益を上回る場合、又は法的な理由により処理が必要な場合、当社は異議があっても個人データの処理を継続することが可能であること。
- データ対象者に関して保有する個人データを破棄するよう Entrust に要請すること。当社は、個人データが処理される目的にとって依然として必要であり、Entrust が処理を継続する法的根拠がある場合、この要請を拒否することが可能であること、
- Entrust に対して、特定の状況下で個人データの処理を保存に制限するよう求めること。

Entrust は、データ保護法に基づくデータ主体の権利を事例ごとに評価し、Data Subject Request（データ主体要求手順）（DSR）に従って要求の履行方法を決定します。一般的に、Entrust は、EU GDPR に基づくデータ主体の権利をすべての要求に応えるためのベースラインとして使用し、データ主体に適用されるデータ保護法の下で利用可能な追加的権利をデータ主体により有利な範囲で適用します。データ主体がこれらの権利を行使し、Entrust が当該個人データを第三者に開示した場合、当社は当該第三者もデータ主体の希望に沿うよう最善を尽くします。

Entrust が保有する個人データに関する情報を要求したいデータ主体は、正式なデータ主体要求（DSR）を提出する必要があります。従業員が直接依頼を受けた場合（口頭ないしは書面）、その依頼は直ちに privacy@entrust.com に転送される必要があります。

9.4 監督当局

関連するデータ監督当局の連絡先は地域によって異なります。欧州データ保護委員会（European Data Protection Board）当局のリストは、こちらを参照してください。英国（UK）情報コミッショナー事務局（ICO）のウェブサイトはこちらを参照してください。カナダ個人情報保護委員会事務局（Office of the Privacy Commissioner of Canada）のウェブサイトはこちらを参照してください。

9.5 データ保護責任者

別段の定めがない限り、Entrust のデータ保護責任者は以下のとおりです：

Mishcon de Reya LLP（ミシュコン・デ・レイヤ法律事務所）
Africa House, 70 Kingsway, London, WC2B 6AH, United Kingdom
DPO@mishcon.com

10. 順守

すべての社員及び臨時従業員は、本ポリシーを遵守することが求められます。さらに、すべての事業部門は、本ポリシー及び各管轄区域で適用されるデータプライバシーの法令を遵守するために、適切な現地基準及び手順が整備されていることを確認しなければなりません。本ポリシー違反は深刻に受け止められ、解雇を含む懲戒処分の対象となる場合があります。本ポリシーはいつでも更新又は修正される可能性があります。

11. 例外

本ポリシーに例外はありません。

12. 所有権と改訂履歴

本ポリシーは、プライバシー担当ディレクターが所有し、毎年見直す必要があります。