ENTRUST

グローバル個人データ保護ポリシー

文書バージョン	1.6
日付	2023 年 9 月 5 日

目次

1. はじめに

Entrust Corporation とその子会社および関連会社（総称して「Entrust」または「当社」）は、データ管理者としての役割において当社の社員、臨時従業員、パートナー、サプライヤー、および顧客の個人データを処理し、データ処理者としての役割において当社の顧客およびそのエンドユーザーの個人データを処理します。Entrust が個人データを処理する場合、当社は法的、契約的、および倫理的義務を遵守し、完全な透明性を持って行います。

2. 目的

本ポリシーは、当社が関連する法的義務および契約上の義務、ならびに認証および監査要件を遵守することを保証するために、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および要素を定めています。本ポリシーは、Entrust が直接行う個人データ処理、および Entrust に代わって個人データを処理する第三者が間接的に行うすべての個人データ処理全体に適用されます。

3. 定義

「**データ管理者**」は個人データ処理の目的および手段を決定する主体を意味し、ISO 27701 の「個人識別情報管理者」と同じ意味を持ちます。

「**データ処理者**」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 の「個人識別情報管理者」と同じ意味を持ちます。

「**データ保護の影響評価**」は、データ管理者またはデータ処理者が、データ処理がデータ対象者の権利と自由に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、EU 一般データ保護規則（GDPR）、英国の個人データ保護に関する国内法（UK GDPR）、カナダの個人情報保護および電子文書法（PIPEDA）、米国プライバシー法を含みますがこれらに限定されない、すべての個人データ保護法および Entrust に適用されるプライバシーに関する法律および規制を意味します。

「**データ対象者**」は個人データに関連する識別された、または識別可能な個人または世帯を意味し、ISO 27701 の「個人識別情報管理者」に帰するものと同じ意味を持ちます。

「**データ移転の影響評価**」は、欧州委員会による適切性認定を受けていない欧州経済地域外の国（すなわち GDPR の対象国）への個人データの移転が与える影響とセキュリティへの影響について、データ管理者またはデータ処理者が文書化した分析を指します。

「**合法的利益影響評価**」は、正当な利潤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、データ管理者またはデータ処理者によって文書化された分析を指します。この評価には、個人データ処理が正当な利潤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、データ対象者の利益が正当な利潤に優先するかどうかの分析という 3 つの要素からなるテストが含まれます。

「**個人データ**」は、データ保護法で定義されている「個人識別情報」、「個人情報」、またはこれらに相当する用語に与えられた意味を持ちます。

「**個人データに関するインシデント**」、「セキュリティインシデント」、「セキュリティ違反」、「個人データ侵害」、またはデータ保護法の下で定義されるこれらの用語と同等の用語に付与される意味を有し、個人データが許可を受けていない者ないしは不正な方法によってアクセス、開示、改ざん、紛失、破壊、または使用されたこと、またはその可能性があることを Entrust が認識する状況を含みます。

「**処理**」とは、収集、記録、組織構造化、保管、適応または変更、検索、相談、使用、送信による開示、普及またはその他の利用可能な状態にすること、整列または結合、制限、消去または破壊など、自動手段であるかどうかにかかわらず、個人データに対して行われるあらゆる操作また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移転または開示も含まれます。

「**個人の機密データ**」は個人データの小集団であり、紛失、欠陥、アクセス、または不適切に開示された場合、データ対象者に危害、困惑、不便、または不公平となる場合があるため、高度な保護の対象とされているデータ対象者に関する情報を指します。

「**特別カテゴリのデータ**」とは個人データの一部であり、個人の人種や人種に関するバックグラウンド、性生活や性的指向、政治的な見解、信条や哲学的な信念、労働組合への参加状況、遺伝子データ、生物学的なデータ（目の色、髪の色、身長、体重など）、病歴、犯罪歴のような情報を示します。

4. 個人データ処理の基本原則

Entrust は個人データを処理する際、以下の基本原則を遵守します。

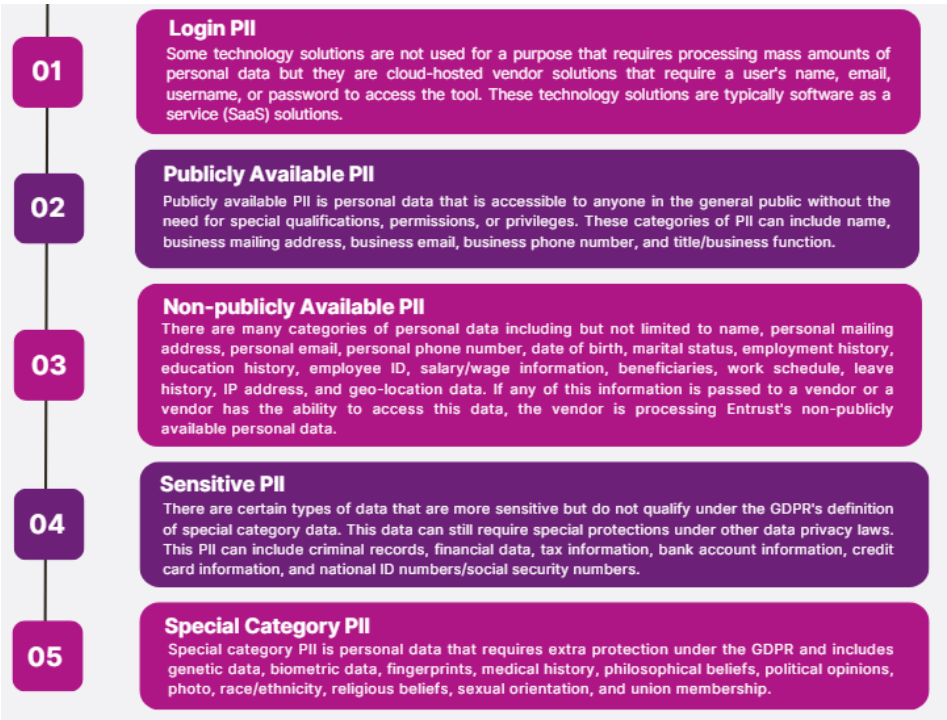
- **合法性と妥当性**：当社は、個人データが合法的な目的のために収集され、その目的に合致し、かつ必要なものであることを保証します。

- **精度と保持**：当社は、システムを常に最新の状態に保ち、不正確な個人データを更新または削除するための仕組みを提供し、処理に対する合法的な目的のため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に安全かつ保護されている状態であることを保証しますが、セキュリティインシデントやデータ侵害が発生した場合には、必要に応じて適時に通知を行うことを含め、迅速かつ適切な対応を行います。
- **透明カード**：当社は、データ対象者の個人データを処理する際に、データ対象者に適切に通知します。その情報を必要とする理由、利用方法、取り扱いおよび保護方法を明確にします。

当社の全員が、個人データを適切に処理して保護する責任を負っており、これを怠れば、Entrust に対する顧客の信頼を損なうだけでなく、当社に多額の罰金や刑罰が科される可能性があることを理解しています。

5. データ分類

Entrust は処理活動の中央記録を保持します。すべての個人情報は、以下のいずれかのカテゴリに分類されます。



6. 合法性と妥当性：

6.1 個人データの処理の法的根拠

当社は、法的に許可され、データ対象者に適切な通知を行った場合にのみ、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いて処理を行います。

- 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、法的義務の遵守、
- データ対象者の利益または基本的な権利および自由が優先される場合を除く、合法的な利潤、および
- 合意。

合意が処理の法的根拠となる場合（マーケティング目的など）、Entrust は、合意が自由に与えられ、具体的で、十分な情報を提供され、データ対象者の希望を明確に示すものであることを保証します。データ対象者は、理由の如何を問わず、いつでも合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 デザインの評価

Entrust は、新規または大幅な変更を行った製品提供の設計・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、ベンダーのクラウド ホスティング ソリューションに実装する際、個人データ処理を基本原則に照らして評価します。プライバシー バイ デザインの評価は Entrust の開発・ベンダー実装プロセスに組み込まれ、コンプライアンスおよび情報セキュリティによってレビューされます。承認を受けずに開発を進めることはできません。

6.2.2 データ保護の影響評価（DPIA）

想定される個人データ処理が個人の権利と自由に深刻なリスクにつながる場合、Entrust は正式な DPIA を完了し、処理の目的、Entrust が関連データ保護法を遵守する方法、当社がデータ対象者の権利に対する潜在リスクの軽減方法を文書化して評価を行います。

6.2.3 データ移転の影響評価（DTIA）

Entrust が欧州経済領域（EEA）外の、欧州委員会による適切性認定の恩恵を受けていない国に個人データを移転する場合、Entrust は、特に、受信国の法律によって転送される個人データへの政府のアクセスが許可される可能性がある場合、転送の影響とセキュリティへの影響を分析するための正式な DTIA を完了します。

6.2.4 合法的利益影響評価（LIIA）

Entrust が個人データ処理の法的根拠として正当な利潤に依拠する場合、当社は正式な LIIA を完成し、正当な利潤を文書化と評価を行って処理の必要性を判断し、データ対象者の権利が正当な利益を上回るかを評価します。

6.2.5 機密データおよび特別カテゴリの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 は社員に代わって、さまざまな業務システムで機密性の高い個人情報を処理し、一部の限定された特別カテゴリのデータを自主的に、かつ現地の法律で許可された範囲で処理します。適切な管理が実施され、適用される DPIA、機密および特別カテゴリのデータのアクセス管理基準、および機密および特別なカテゴリのデータを取り扱う社員に対する強化されたプライバシー研修に概説されています。

6.3 契約上の保護

6.3.1 グループ内のデータ移転協定（IGDTA）

Entrust グループ内の会社（すなわち、すべての企業体および子会社）は、EEA 域外かつ Entrust グループ内で欧州委員会による適切性認定の恩恵を受けていない国に個人データを移転する際、適切な保護措置を確実に講じることを目的として、グループ内データ移転契約を締結します。

6.3.2 データ処理契約（DPA）

Entrust のために、または 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（例えば、ベンダー、サプライヤ、チャネル パートナー）が関連データ保護法を遵守するための適切な技術的・組織的措置を確実に講じるため、Entrust とデータ処理契約を締結する必要があります。Entrust が標準的な顧客 DPA を通じてデータ処理者として行動する場合は、同等の取り組みを行います。

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、サプライヤー、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。

7. 精度と保持

7.1 役割管理

グローバルな記録管理プログラムでは、個人データを必要な期間だけ保管するために、個人データの処理について保管期間が正式に定義され、指定された保管期間の終了時に個人データが消去、破壊、または匿名化されるようにします。グローバル記録管理ポリシーは、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、付属の記録保持スケジュールには当社が保持する記録の種類ごとに保持期間が定められています。

7.2 個人データの保管とバックアップ

Entrust は、当社が直接およ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 部門および関連ベンダー（IT 部門以外が管理するクラウド・ホスティング・アプリケーションの場合）には、ストレージや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ガイダンスが提供されます。

Entrust は、商業的に実行不可能な場合、保存期間終了時にバックアップメディアおよびサーバから個人データのコピーを削除しません。ただし、Entrust がこのような方法で保持する個人データは、使用中の個人データ保護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秘密保持の対象となるため、適用法で要求される場合を除いてアクセスすることはできません。

7.3 個人データの消去または廃棄

グローバル記録管理ポリシーおよび情報分類取扱基準は、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適切に処理するための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、個人データをコピーしてはならず、コピーしたものには元の機密または所有権に関する表示を保持する必要があります。

- 紙の記録は、保管する必要が消失した場合はシュレッダーにかけて、安全に廃棄する必要があります。
- 電子形式の個人データは、不要になった時点で削除または匿名化する必要があります。
- IT 部門は、関連する情報セキュリティポリシーおよび基準に従って、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機器、BYOD（私物携帯機器の業務使用）デバイス上の業務データなど）を破棄また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所には、個人データの安全性を確保し、不正または違法な処理、偶発的な損失、破壊または損害から保護するための適切な措置を講じます。以下のようにして、Entrust はこれを実現します。

- 法律または契約により要求され、さらに商業的に実行可能な場合には、静止時および転送時に個人データを暗号化、
- 定期的に試験または演習される正式な事業復旧および災害復旧計画を通じて、個人データ処理に使用されるシステムおよびサービスの継続的な機密性、完全性、可用性、および回復力を確保、
- 物理的または技術的な事故が発生した場合に、個人データへのアクセスをタイムリーに回復することを保証、
- 個人データの保護を目的として実施されている技術的および組織的措置の有効性を定期的にテスト、評価、判断、
- 物理的なセキュリティ基準の実施、机や戸棚に個人情報がある場合は施錠、個々のモニター/画面が通行人から個人情報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）は放置する場合は施錠、会社のシステムからログオフすることを義務付けています。

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または違法な破壊、紛失、改ざん、不正な開示、また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、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・組織的措置を実施する契約規定（DPA など）に従うものとします。このような仕組みがない場合、個人データが Entrust 社外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）を導入して、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

事前に正式なセキュリティ例外 の承認がない限り、個人データを 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、本番環境で実施されている現行の基準および管理に従う必要があり、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、テスト終了後に遅滞なく削除されなければなりません。 詳細については、セキュアソフトウェア開発ライフサイクル（S-SDLC）に概説されています。

8.3 個人データに関するインシデントの報告

個人データに関するインシデントは、以下のようなさまざまな形で発生する可能性がありますが、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 Mobile Device またはハードコピーファイルの紛失（例：公共交通機関に誤ってデバイスを置き忘れる）、
- 個人情報を含むモバイル機器やハードコピーファイルの盗難、
- 人為的ミス（例：社員が個人データを含む電子メールを意図しない受信者に誤って送信したり、個人データを誤って変更または削除したりすること）、
- サイバー攻撃（例：ランサムウェアやその他のマルウェアを含む未知の第三者からの電子メールの添付ファイルを開くこと）、
- 不正な使用/アクセスを許可する（例：権限のない第三者に Entrust のオフィスまたはシステムの安全な領域へのアクセスを許可すること）、」
- 物理的な破壊や損失（火災や洪水など）、または
- 第三者が詐欺（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します。

以下がある場合、個人データインシデントが発生した可能性のある兆候には以下のものがあります。

- アクティブなユーザアカウントに関して、異常なログインおよび/または過剰なシステム活動。
- 異常なリモートアクセス活動。
- Entrust の作業環境から見える、またはアクセスできる偽装無線（Wi-Fi）ネットワークの存在。
- 機器の故障、または
- Entrust のシステムに接続された、またはインストールされたハードウェアまた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、または発生しつつあることに気付いた、またはそう疑う理由がある社員は、直ちに Entrust のセキュリティオペレーションセンター（SOC@entrust.com）に連絡する必要があります。

8.4 個人データに関するインシデントへの対応

個人データに関するインシデントが実際に発生した場合、または発生が差し迫った場合、Entrust は情報セキュリティにより維持されている事故対応・処理手順を実施し、事故の影響を最小限に抑え、法律上および/または契約上の要求に応じて、規制当局、データ対象者および/またはその他の関係者に通知します。回答には通常、以下が含まれます。

- 結果として生じる、または生じた可能性のある損害または被害の性質、原因および程度を判断するために、事件を調査する、
- インシデントの継続または再発を阻止し、影響を受けるデータ対象者への被害を限定するために必要な措置を実施する、
- 他の当事者（各国のデータ保護当局、影響を受けるデータ対象者、契約上の当事者）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、また
- 規制当局または影響を受ける当事者に通知するか否かの決定を文書化することを含め、個人データに関するインシデントおよ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 および外部 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、データ管理者およ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対象者に通知します。この情報は、ウェブユーザ、求職者、社員向けの Entrust の各

種プライバシー通知、およ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。このような通知は、以下のような情報を提供します。

- Entrust が処理する個人データの種類、
- 処理の目的と法的根拠、
- 処理に使用される第三者（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た移転、
- 処理期間、
- データ対象者の権利、および
- 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、社員に対して、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ています。この「データプライバシー入門トレーニング」は、入社時およびその後も毎年的に行われます。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、機密データや特別カテゴリの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 は引き続き必要に応じて、職務に特化したプライバシー・トレーニングを開発および展開していきます。

9.3 データ対象者の権利

Entrust が個人データを処理する場合、データ対象者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、データ対象者は一般的に以下の権利を有します。

- 自分に関する保有個人データの情報を請求する権利、
- 自分に関する不正確な個人データを訂正し、不完全な個人データを完了させること、
- 当社が自らの正当な利潤を追求するために個人データを処理している場合、Entrust が個人情報を処理することに異議を唱える権利。ただし、当社の正当な利潤がデータ対象者の利益を上回る場合、または法的根拠のために必要な場合は、異議申し立てにかかわらず個人データの処理を継続することが可能です。

- データ対象者に関して保有している個人データを破棄するように Entrust に依頼する権利。個人データが処理されている目的のためにまだ必要であり、Entrust が処理を継続する法的根拠がある場合、当社はこの要求を拒否することができます。
- 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 Entrust に依頼します。

Entrust は、データ保護法に基づくデータ対象者の権利をケースバイケースで評価し、データ対象者の要求手順に従って要求の履行方法を決定します。基本的に、Entrust はデータ対象者の権利を、すべての要求に応じるための根拠として EU GDPR に従っており、データ対象者に適用されるデータ保護法規に従って利用可能な追加の権限をデータ対象者にとってより有利となる範囲で適用します。データ対象者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対象者の希望を遵守するように最善を尽くします。

Entrust が保有している個人データに関する情報を希望するデータ対象者は、正式なデータ対象者要求（DSR）を提出することで情報を得ることができます。社員が直接依頼を受けた場合（口頭であれ書面であれ）、その依頼は直ちに privacy@entrust.com に転送しなければなりません。

9.4 監督当局

関連するデータ監督当局の連絡先は拠点ごとに異なります。EU のデータ保護委員会当局一覧についてはここを参照してください。英国（UK）個人データ保護監督機関（ICO）のウェブサイトはこちらからご覧ください。カナダのプライバシー委員長オフィスはここを参照してください。

10. コンプライアンス

すべての社員および臨時従業員は、このポリシーを遵守することが求められます。さらに、すべてのビジネスユニットは、本ポリシーおよび管轄地域で適用されるデータプライバシー法を遵守するために、適切な現地の基準および手順を設けなければなりません。本ポリシーに違反した場合は、深刻に受け止められ、解雇を含む懲戒処分の対象となることがあります。本ポリシーは、いつでも更新また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. 所有者およびレビュー

本ポリシーは最高法務およびコンプライアンス責任者が所有し、毎年見直されるものとします。

12.1 連絡先情報

本ポリシーまたは Entrust の個人データの取扱いに関するご質問は、privacy@entrust.com までご連絡ください。