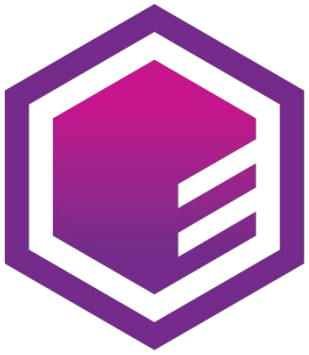

ENTRUST

グローバル個人データ保護ポリシー

文書バージョン	1.4
日付	2021年12月10日

目次

1. はじめに

事業者および雇用者として、Entrust Corporation とその子会社および関連会社（以下、総称して「Entrust」または「当社」という）は、当社の従業員、臨時従業員、顧客、サプライヤー、および当社に代わって製品またはサービスを提供するために契約しているその他の第三者に関する個人データを収集、保管、処理する必要があります。

2018年5月25日の EU 一般データ保護規則（以下、「GDPR」という）の導入およびデータ保護を規定するその他の適用法により、当社は、個人データの収集、使用、保存の方法に関する強化された要件の対象となります。

2. 目的

本ポリシーの目的は、当社が法的義務を遵守し、当社が個人データを保有する個人が当社に対して信頼を寄せることができるようにすることです。 本ポリシーは、Entrust の全従業員、臨時従業員、および Entrust に代わってデータを処理する第三者に適用されます。 特に定めのない限り、本ポリシーは、特に明記されていない限り、Entrust が事業を展開しているすべての国で適用されます。

3. ポリシーの要件

3.1 定義

「データ管理者」または**「個人識別情報管理者（PII 管理者）」**とは、個人データの処理の目的および手段を決定する事業者を意味します。

「データ処理者」または**「個人識別情報処理者（PII 処理者）」**とは、管理者に代わって個人データを処理する事業者を意味します。

「データ保護法」とは、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及び電子文書法（PIPEDA）、カリフォルニア州消費者プライバシー法（CCPA）を含みますがこれらに限定されない、適用されるすべてのデータ保護およびデータ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」または**「個人識別情報主体（PII 主体）」**とは、個人データが関連する、識別された、または識別可能な個人または世帯を意味します。

「データ利用者」とは、従業員、コンサルタント、独立契約者、インターン、派遣社員、または Entrust のために個人データを処理する業務を行う第三者（データ処理者を含む）を表す用語です。

「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」、「個人データ」またはこれらに相当する用語に与えられた意味を持つものとします。

「個人データに関するインシデント」とは、データ保護法により「セキュリティインシデント」、「セキュリティ侵害」または「個人データ侵害」という用語に付与された意味を持つものとし、ベンダーが、個人データが権限のない者によって不正な方法でアクセス、開示、改ざん、紛失、破壊または使用されたか、その可能性があることを認識するあらゆる状況を含むものとします。

「処理」とは、収集、記録、組織化、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。

「特別カテゴリーデータ」または**「特別カテゴリー個人情報」**とは、個人データのサブセットであり、個人の人種または民族的出身、性生活または性的指向、政治的意見、宗教的または哲学的信念、労働組合への加盟、遺伝データ、生体データ（目の色、髪の色、身長、体重）、病歴、または犯罪歴や犯罪行為、あるいは関連するセキュリティ対策に関する情報を指します。

3.2 当社の責任

状況に応じて、Entrust　はデータ管理者またはデータ処理者として行動することができます。データ管理者である Entrust は、データ保護法に沿った実務とポリシーを確立する責任があります。　Entrust がこれらの法律を遵守していることを証明できることも同様に重要です。 当社はこれを以下のように行います。

- 本ポリシー、文書の保持およびデータセキュリティに関するポリシー、Entrust　のプライバシー文書など、会社がデータ保護法を遵守することを可能にするポリシーを実施する。
- データ保護要件について、従業員、臨時従業員、および Entrust を代表して行動する第三者に連絡し、教育する。
- Entrust　のデータ保護ポリシーへの違反事例を調査し、適切な是正措置や懲戒処分を行う。
- 個人データに関するインシデントの調査、修復、場合によっては通知を行う。
- 新しいタイプの処理活動に必要な場合、データ処理の影響評価を実施する。
- Entrust のデータ保護ポリシーおよび手順に関する定期的な内部監査を実施する。
- 新製品の設計時にデータ保護を考慮する。

3.3 個人データの取り扱いについて

当社が処理する、または Entrust に代わって処理される個人データは、以下のとおりでなければなりません。

- 公正、適法、かつ透明性のある方法で処理されること。
- 指定された明確かつ合法的な目的のためにのみ処理されること。
- データが処理される正当な目的のために必要なものに限定し、関連性を持たせること。
- 正確かつ最新の状態に保ち、合理的に可能であれば、不正確な個人データを遅滞なく消去または修正すること。
- データを収集した目的を果たすために、必要な期間を超えて保持しないこと。
- 不正または違法な処理、偶発的な損失、破壊または損傷からの保護を含む、個人データの適切なセキュリティを確保する方法で処理されること。

3.4 機密情報および特別なカテゴリーのデータ処理

Entrust は、同役に代わって様々なビジネスシステムで機密情報を処理し、Workday では限定された特別なカテゴリーのデータを処理します。　適切な管理が行われており、「特別なカテゴリーのデータ」、「給付金と給与」の DPIA、および 「機密性の高い特別なカテゴリーのデータのための Access Control Standard」（Entrust Compliance のサイトで入手可能）に概説されています。

3.5 個人データの処理の法的根拠

当社は、データ保護法に基づいて許可された場合にのみ、個人データを処理することができます。 以下は、Entrust が個人データを処理する際に依拠する根拠です。

処理が必要な場合

- データ対象者が当事者である契約の履行のため、または契約締結前にデータ対象者の要請に応じて措置を講じるため。
- 法執行当局からの法的請求に限らずこれを含むEntrustが従うべき法的義務の履行、または
- Entrust　の正当な利益を追求するため。ただし、かかる利益がデータ対象者の利益または基本的な権利および自由に優先する場合を除く。

これらの理由に加えて、Entrust は、データ対象者が1つまたは複数の特定目的のための処理に同意した場合にも、個人データを処理することができます。ただし、同意が自由に与えられ、具体的で、情報を与えられ、データ対象者の希望が明確に示されていることが条件となります。 Entrust が同意を処理の根拠としている場合、データ対象者はいつでも、どのような理由でも同意を撤回する権利があります。

Entrust　は、顧客、従業員または臨時従業員の特別なカテゴリーの個人データを処理する必要がある場合もあります（例：安全な雇用慣行で必要な場合）。 Entrust が特殊なカテゴリーの個人データを処理する場合、または第三者を利用して処理を代行する場合、Entrust　は該当する場合に、以下の条件が満たされていることを確認します。

- データ対象者が、1つまたは複数の特定目的のために特別なカテゴリーの個人データを処理することに明示的に同意したこと。
- 雇用法、社会保障法、社会保護法、または団体協約に基づく義務を遂行するために必要な処理を行うこと。
- 予防医学や産業医学の目的、または従業員の労働能力の評価のために処理が必要であること。
- データ対象者が物理的または法的に同意を与えることができない場合に、データ対象者または他の人の重要な利益を守るために処理が必要であること。
- データ対象者によって公開された個人データに関連する処理を行うこと。
- 法的主張を確立または弁護するために必要な処理を行うこと。

3.6 データ記録の管理

Entrust は、当社が収集する個人データの種類と、そのデータを収集する理由を記録しています。 Entrust は、記録に記載された特定の目的またはデータ保護法で認められたその他の目的のためにのみ、個人データを処理します。 Entrust は、データを最初に収集した時、またはそれが不可能な場合はその後可能な限り早く、データ対象者にその目的を通知します。

当社は、データ対象者に提供した目的に必要な範囲でのみ個人データを処理します。 つまり、必要以上の個人データを要求したり、システムに記録したりすることはありません。 当社は、必要でなくなった個人データを確実に消去または破壊するために、適切な技術的および組織的措置を講じています。

また、保有する個人データを正確かつ最新の状態に保つための合理的な措置を講じています。 Entrust は、あらゆる個人データの正確性を、収集時点およびその後の定期的なチェックを行うことを目指しています。 当社は、不正確なデータまたは古いデータを不当に遅延することなく、いかなる場合でもデータ対象者の要求から1ヶ月以内（1ヶ月が不可能な特定の理由がある場合は最大3ヶ月間）に消去、破棄、または修正するためのあらゆる合理的な手段を講じます。

記録の管理と保持についてさらに詳しいことは グローバル記録の管理ポリシーと付属文書記録の保持スケジュールをご参照ください。

3.7 個人データの消去または廃棄

個人データを含む紙の記録は、保持する必要がなくなった時点でシュレッダーにかけ、安全に廃棄しなければなりません。 *個人データを含む紙の記録は、それ以外の方法で廃棄することはできません。*

電子的な個人データを削除する際には、問題のデータを使用できないようにするために、可能な限りの措置を講じる必要があります。　個人データを完全に削除することが不可能な場合は、データを可能な限り削除するための合理的な措置を講じなければなりません。

IT 部門は、個人データを含む電子機器（ノートパソコン、デスクトップ、会社所有の Mobile Device、BYOD 機器の業務データなど）を廃棄または消去する責任があります。

3.8 情報セキュリティ

当社が個人データを処理する際には、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合理的な措置を講じます。　以下のようにして、Entrust はこれを実現します。

- 可能かつ適切な場合、個人データを暗号化する。
- 個人データを処理するため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する。
- 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する。
- データセキュリティを確保するための技術的・組織的措置の有効性のテスト、評価、査定を促進する。

適切なセキュリティレベルを評価する際、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委託する場合、当該第三者は書面による指示に基づいて行い、守秘義務を負い、データセキュリティを確保するために適切な技術的および組織的措置を実施する義務を負います。 個人データは、Entrust または認定された第三者以外の者と共有することはできません。

机や戸棚に個人データや機密情報が入っている場合は、鍵をかけておきます。　データ利用者は、個々のモニター/スクリーンが個人データや機密情報を通行人に見せないようにし、放置されたコンピュータ/タブレットをログオフするかロックするようにします。

3.9 個人データに関する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方法で起こり得ます。

- 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）。
- 個人データを含む Mobile Device またはハードコピーファイルの盗難（例：車や家から盗まれる）。

- 人為的ミス（例：従業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）。
- 火事や洪水などの不測の事態。
- 第三者が偽装して Entrust から情報を入手する。

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。

- 特に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。
- 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、または発生しそうだと気付いた同僚は、直ちに Entrust Security Operation Center（電子メール：SOC@entrust.com）およびコンプライアンスディレクター（電子メール：privacy@entrust.com）に連絡しなければなりません。

3.10 個人データインシデント対応計画

実際に個人データに関するインシデントが発生した場合、または差し迫ったインシデントが発生した場合、Entrust はインシデントの影響を最小限に抑えるために迅速な行動をとり、法律によって要求される場合はインシデントを報告します。 ほとんどの場合、その対応は以下のとおりです。

- 結果として生じる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、それらの通知を行う。 データ保護当局への通知義務がある場合、報告は通常、当社（いずれの従業員をも含む）がインシデントを認識してから 72 時間以内に行う。

- 通知するかしないかの判断を説明する文書を含め、個人データに関するインシデントに関する情報および対応措置を記録する。

3.11 個人データの保管とバックアップ

Entrustは個人データの保管とバックアップ用のサーバーを複数拠点で利用しています。Entrustが同僚と顧客に代わり個人データを処理するために委託している第三者が利用するサーバー拠点については、同僚の個人データに関する関連データの保護影響評価および社外の請負データ処理者のページおよび顧客の個人データを対象とする製品のプライバシーに関する注意を参照してください。　これらの全文書は社内ではコンプライアンスページに、社外ではデータプライバシーのアイコン下にある法務およびコンプライアンスサイトに保管されています。　現在の本社データサーバー拠点リストは同僚が直接IT部署に問い合わせることもできます。

3.12 国際的なデータ移転および第三者への移転

GDPR に基づき、Entrust は、欧州経済領域（以下、「EEA」という）外の国で十分な保護水準が確保されている場合、または Entrust がデータ保護を確保するための適切な措置を講じている場合に、個人データを移転することができます。

Entrust グループ内の企業（すべての法人および子会社）は、EEA 外ではありますが Entrust グループ内での個人データの転送に対する適切な保護を確保するために、「グループ内データ転送契約」を締結しなければなりません。

Entrust がデータ管理者またはデータ処理者として機能する Entrust のために、または Entrust に代わって個人データを処理する Entrust グループ外の企業は、EEA 域外への個人データの転送に対する適切な保護措置を確保するために、Entrust　とデータ処理契約を締結しなければなりません。　その契約書には、第三者が GDPR を遵守し、データ主体の権利を確実に保護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文言が含まれています。

Entrust が個人データを EEA 外の国に移転する例としては、以下が考えられます。

- データ対象者が、Entrust　が当該移転に関連する可能性のあるリスク（当該国に同等の保護措置がないことなど）を通知した後、提案された移転に明示的に同意した場合。
- データ対象者が当事者である契約を履行するため、または契約締結前にデータ対象者の要求に応じて措置を講じるために移転が必要な場合。
- データ対象者が物理的または法的に同意を与えることができない場合に、データ対象者または他の人の重要な利益を保護するために転送が必要な場合。
- 法的請求の確立または防御のために転送が必要な場合。

EEA 域外へのデータ転送については、Entrust は欧州委員会が定めた標準契約条項（2001/497/EC、2004/915/EC、2010/87/EU）に依拠します。[1] なお、カナダ国外に個人データを転送する場合は、データ転送契約が必要となります。

3.13 データ対象者への通知

Entrust は、データ対象者の個人データの処理について、データ対象者に情報を提供する必要があります。 この情報は、www.entrust.com で公開されている当社のウェブプライバシー文書、https://www.entrust.com/legal-compliance/data-privacy/job-applicant-privacy-statement で公開されている求職者のプライバシー文書、および Entrust のイントラネットで公開されている従業員のプライバシーポリシーに含まれています。 このような文書は、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。
- 個人データを処理する目的と法的根拠。
- 処理の過程で個人データが第三者に開示されるかどうか。
- 個人データが EEA およびカナダ以外の国に転送されるかどうか、転送される場合はどのような保護措置が講じられるか。
- 個人データの処理期間、または判断できない場合は、当社が処理期間を決定するために使用する基準。
- データ対象者が Entrust が保有する自分の個人データの写しを入手する方法。
- 苦情を申し立てる方法を含む、データ対象者の権利。
- 法律または契約を遵守するために個人データを処理しなければならない場合、データ対象者がデータを提供しない、または処理に異議を唱えない場合に起こりうる結果。
- 該当する場合は、自動化された意思決定プロセスの存在と詳細。

Entrust がデータ対象者に関する個人データを第三者から受け取る場合、当社はデータ対象者に以下の情報も提供します。

- 第三者から受け取った個人データの種類。
- データの出所、および一般にアクセス可能な出所（一般にアクセス可能なウェブサイトなどから来たものかどうか）。

3.14 プライバシーバイデザインとデータ保護影響度評価

[1] 2022年12月27日以降、これらの移転は、欧州議会および欧州理事会の規則（EU）2016/679に基づく個人データの第三国への移転のための標準契約条項に関する2021年6月4日の欧州委員会実施決定（EU）2021/914に概説されている新しい標準契約条項を用いて行われます。

データ保護法により、Entrust は新製品の開発段階でデータ保護を考慮する必要があります。この義務を果たすために、Entrust はデータ保護を設計プロセスの一部とし、個人データの収集を可能な限り最小限に抑えるための手段を講じなければなりません。

状況によっては（すなわち、処理が個人の権利と自由に高いリスクをもたらす場合）、Entrust は個人データの処理に関連して正式なデータ保護影響評価（DPIA）を実施する必要があります。 このような評価では、活動を行う目的、Entrust がデータ保護法をどのように遵守するか、当社が個人のプライバシー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ます。 データ保護影響評価が必要であると思われる場合は、コンプライアンスディレクター（privacy@entrust.com）までご連絡ください。

3.15 データ対象者の権利

Entrust が個人データを処理する場合、データ保護法に基づき、データ対象者は以下の権利を持つことができます。

- 自分に関する保有個人データの情報を請求する権利。
- データが実際には不正確または不完全であると Entrust が判断することを条件に、自分に関する不正確な個人データを修正し、不完全な個人データを補完する権利。
- 当社が自らの正当な利益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、当社の正当な利益がデータ対象者の利益を上回る場合、または法的請求の確立または弁護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できる。
- 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 が処理を継続する正当な根拠がある場合、当社はこの要求を拒否することができる。
- 個人データの処理を保管に限定するように Entrust に依頼する権利。 これは、個人データの正確性が争われ、検証されていない場合、Entrust が個人データを必要としなくなったが、データ対象者が法的請求を確立または弁護するために個人データを必要とする場合、データ対象者が個人データの処理に異議を唱えた場合、Entrust がその正当な利益がデータ対象者の利益を上回るかどうか、または処理が違法であるかどうかを判断している場合にのみ要求できる。

Entrustは適用されるデータプライバシー法規に従ってケースバイケースでデータ対象者のアクセス依頼に応える方法を決定するためにデータ対象者の権利を評価します。 基本的に、Entrustはデータ対象者の権利を要求に応じるための根拠としてEU GDPRに従っており、適用されるデータ保護法規に従って利用可能な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。

3.16 データ対象者のアクセス権

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、データ対象者アクセス要求（DSAR）を提出することで情報を得ることができます。 同僚が直接依頼を受けた場合（口頭、書面を問わず）、直ちに依頼の詳細を privacy@entrust.com に転送してください。 管轄地域別データ対象者の権利一覧はコンプライアンスサイトにあるデータ対象者のアクセス要求手順を参照してください。

3.17 トレーニング

Entrust は、従業員および臨時従業員にデータ保護の責任に関するトレーニングを提供します。 このトレーニングは、入社時およびその後も定期的に行われます。

3.18 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。 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。

3.19 データ保護担当者

Entrust のプライバシー情報管理システムについてご質問がある場合は、次の連絡先にお問い合わせください。

Entrust Corporation

注意： Jenny Carmichael、コンプライアンス ディレクター

1187 Park Place

Shakopee, MN 55379

privacy@entrust.com

Entrust Deutschland GmbHが任命したデータ保護担当者は、Althammer & Kil GmbH & Co.社のNiels Kill氏です。 （kontakt-dsb@althammer-kill.de）

4. コンプライアンス

すべての従業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。

5. 例外

本ポリシーに例外はありません。

6. 所有者およびレビュー

本ポリシーの所有者は最高法務およびコンプライアンス責任者です。　本ポリシーは、毎年見直しを行うものとします。　　本文書への変更は、情報セキュリティマネジメントシステム（ISMS）の「文書および記録管理基準」に従うものとします。

6.1 連絡先情報

本ポリシーに関するご質問や、個人データの取り扱いに関する苦情は、コンプライアンスディレクター（privacy@entrust.com）までご連絡ください。

6.2 文書プロパティと改訂履歴

文書プロパティ	
プロパティ	説明
配布	社内外での使用
分類	公開
文書所有者	Lisa Tibbits、最高法務およびコンプライアンス責任者
次回のレビュー予定	2022

文書承認		
承認者名	役職	日付
Lisa Tibbits	最高法務およびコンプライアンス責任者	2019年3月3日
ポリシー管理委員会	該当なし	2021年8月3日
ポリシー管理委員会	該当なし	2021年12月16日

改訂履歴			
バージョン	日付	変更内容	改訂者
1.0	2019年4月19日	初版	Anjali Doherty, Sr. 顧問弁護士 Jenny Carmichael、コンプライアンス ディレクター
1.1	2020年4月19日	年次更新	Anjali Doherty, Sr. 顧問弁護士

			Jenny Carmichael、コンプライアンス ディレクター
1.2	2020年9月10日	新しいポリシーテンプレートに更新	Aileen Havel、シニア コンプライアンス スペシャリスト
1.3	2021年7月6日	年次改訂、特別なカテゴリーのデータへのアクセスに関するセクションの追加	Aileen Havel、準顧問弁護士、Lee Jones、シニア コンプライアンス アシュアランス スペシャリスト
1.4	2021年12月10日	ISO 27701の管理および外部リスクアセスメントに関する勧告に準拠するための更新	Jenny Carmichael、コンプライアンス ディレクター