ENTRUST

グローバル個人データ保護ポリシー

ドキュメントバージョン	1.2
日付	2020 年 9 月 10 日

コンテンツ

1. はじめに

Entrust Corporation、その子会社および協力会社（以下総称して「Entrust」または「会社」）は、企業として、雇用主として、従業員、臨時社員、顧客、サプライヤー、および会社の代わりに製品やサービスを提供す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。

欧州一般データ保護規則（以下、「GDPR」）が 2018 年 5 月 25 日に、またその他の関連するデータ保護法が発効する中、会社が個人データを収集、使用、保管するための要件がより厳格になっています。

2. 目的

このポリシーの目的は、私たち全員が法的責任を遵守し、皆様が会社に個人データを安心して預けられるようにすることです。 Entrust の従業員、臨時社員、および Entrust の代わりにデータを処理する第三者すべてがこのポリシーの対象になります。 別途明記しない限り、このポリシーは Entrust が事業展開および/またはビジネスを行うすべての国において適用されます。

3. ポリシーの要件

3.1 定義

「データ管理者」とは、個人データ処理の目的および手段を決定する組織のことです。

「データ処理者」とは、管理者の代理として個人データを処理する組織のことです。

「**データ保護法**」とは、欧州一般データ保護規則（GDPR）、カナダの個人情報保護および電子文書法（PIPEDA）、カリフォルニア州消費者プライバシー法（CCPA）を含み、これに限定されない関連するすべてのデータ保護法、データプライバシー法や規制のことです。

「データ主体」とは、個人データと紐づく、特定された個人または特定可能な個人や家族のことです。

「データ使用者」とは、あらゆる従業員、コンサルタント、独立契約者、インターン生、臨時従業員や、Entrust の代理として行動し、Entrust のために個人データを処理する第三者（データ処理者を含む）を示す用語です。

「**個人データ**」は、「個人を特定できる情報」、「個人情報」、「個人データ」、データ保護法によって定められている同様の用語の意味に基づきます。

「**個人データのインシデント**」とは、データ保護法における「セキュリティインシデント」、「セキュリティ侵害」、「個人データ流出」という用語が意味するものであり、不正な人物が不正な方法で個人データにアクセスした、データを公開した、改ざんした、データが紛失した、

破壊された、使用された、あるいはその可能性が高いということをベンダーが把握しているあらゆるケースがこれに該当します。

「処理」とは、収集、記録、編さん、保管、編集または改変、取得、コンサルテーション、使用、移転による公開、配布やその他の方法で利用可能にすること、調整や合成、制限、削除や破壊など、自動的な方法かどうかに関わらず、個人データに対して行う作業、または一連の作業のことです。 第三者に対して個人データを移転または公開することも処理に該当します。

「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）、病歴、犯罪歴やそれに関連する安全措置のような情報を示します。

3.2 会社の責任

状況に応じて、Entrust はデータ管理者またはデータ処理者となります。 Entrust はデータ管理者として、データ保護法に則った慣行およびポリシーを確立する責任を負っています。 Entrust がこのような各法律に準拠する形で事業を行うことも同じように重要です。 会社は次のようにしてこれを達成します：

- このポリシー、ドキュメントの保管およびデータのセキュリティに関するポリシー、Entrust のプライバシーに関する声明を会社が遵守できるようなポリシーを作成すること、
- 従業員、臨時社員、Entrust の代理として行動する第三者に対してデータ保護の要件を伝え、トレーニングを行うこと、
- Entrust のデータ保護ポリシーに対する違反を調査し、適切な是正措置および/または懲戒処分を行うこと、
- 個人データのインシデントを調査し、それに対応し、また一部の場合はそれに関する通知を行うこと、
- 新しい種類の処理活動について必要な場合はデータ処理の影響評価を行うこと、
- Entrust のデータ保護ポリシーおよび手順に対する内部監査を定期的に行うこと、
- データ保護を第一に考えて新製品を設計すること。

3.3 個人データの処理

会社処理する個人データ、または Entrust の代理として処理される個人データはいかなるものであっても次の条件を満たす必要があります：

- 公正、合法的かつ透明な形で処理されること、
- 指定された、明示的かつ合法的な目的のためにのみ処理されること、

- データ処理　を行う正当な目的に沿った形で、関連性があり、限定された仕方で処理されること、
- 不正確な個人データは、合理的に可能な限り遅滞なく消去または修正されるように、正確かつ最新の状態に保たれること、
- データを収集するに至った目的を達成するために必要な期間を超えて保管されないこと、
- 不正または違法な処理、予期せぬ紛失、破壊、破損の防止など、個人データのセキュリティを適切に確保して処理されること。

3.4 個人データを処理する法的根拠

会社は、データ保護法によって許されている範囲内でのみ個人データを処理することがあります。 Entrust は、次のような根拠に基づいて個人データを処理します：

処理が必要な場合：

- データ主体との契約を履行するため、または契約締結前にデータ主体の求めで発生する措置を講じるため、
- Entrust が従う法的義務を履行するため、および/または
- データ主体の基本的な権利および自由が Entrust の利害よりも優先される場合を除き、会社が正当な利害を追求するため。

これらの根拠に加え、データ主体が適切な情報に基づいて自由な判断で具体的な同意を明確に自ら行っている場合に、Entrust はその目的のために個人データを処理することもあります。 Entrust が同意を根拠として処理を行う場合、データ主体はいつでも、どのような理由でも同意を撤回する権利を持っています。

また、従業員や臨時社員のために、Entrust が特別カテゴリの個人データを処理しなければならないこともあります（例：職場の安全性に関する要件がある場合）。 Entrust が特別カテゴリの個人データを処理する、または第三者に代わりに処理してもらう際、Entrust は適切な場合に次のような条件に従います：

- 単一または複数の具体的な目的のために特別カテゴリの個人データを処理することについて、データ主体から明示的な同意を得ること、
- 雇用法、社会保障、社会的保護の法律、団体協約に基づく義務を遂行するために処理が必要であること、
- 予防医学や職業医学のために、または従業員の業務キャパシティを評価するために処理が必要であること、
- データ主体や、データ主体が身体的または法的な理由で同意を行えない場合は別の人物の不可欠な利害を守るために処理が必要であること、
- データ主体が公開した個人データに関連する処理を行うこと、および/または
- 法的主張を確立または弁護するために処理が必要であること。

3.5 データの記録管理

Entrust は、収集する各種の個人データおよびデータを収集する理由を一元的な記録を保持します。 中央の記録に示されている特定の目的、またはデータ保護法が許可しているその他の具体的な目的のため以外に、Entrustが個人データを処理することはありません。Entrustは、データを最初にする際や、それが不可能な場合は収集後、速やかにデータ主体にその目的を通知します。

Entrust は、データ主体に示した目的を達成するために必要となる最小限の範囲でしか個人データを処理しません。 つまり、Entrustが必要以上に個人データを求めたり、システムに記録を残したりすることはできません。 会社は、不要になった個人データを必ず削除、破壊できるよう、適切な技術および組織的な対策を用意しています。

会社はまた、個人データの正確さと最新性を維持するために、合理的な対策も行っています。Entrust は、個人データの収集時、およびその後定期的に個人データの正確さをチェックするように努めています。 会社は速やかに、遅くともデータ主体の要求後 1 か月（または、1か月では不可能という具体的な理由がある場合は最長3か月）以内に不正確または古くなったデータを削除、破壊、修正するために、あらゆる措置を講じます。

3.6 個人データの削除や破壊

個人データが含まれる紙媒体の記録は、データを保管する必要がなくなった際に、シュレッダーにかけて安全な形で廃棄する必要があります。 *個人データが含まれる紙媒体の記録を他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は、対象のデータを使用できなくするために可能な限りあらゆる手続きを踏む必要があります。 個人データを完全に削除できない場合、できるだけ完全にデータを削除するための合理的な手続きを踏む必要があります。

個人データが含まれる電子機器（例：ノートパソコン、デスクトップパソコン、会社所有のモバイル機器、社員が持ち込んだデバイス内の業務データ）を破壊またはデータ消去する責任は、IT 部門が負っています。

3.7 情報セキュリティ

個人データを処理する際、データのセキュリティを確保し、不正または違法な処理、予期せぬ紛失、破壊、破損を防止するために、会社は合理的な対策を行います。 Entrust は次のような手段でこれを達成します：

- 可能かつ適切な場合は個人データを暗号化すること、
- 個人データを処理するために使用するサービスおよびシステムの機密性、整合性、可用性、回復力を維持すること、

- 物理的または技術的なインシデントが発生した場合、速やかに個人データにアクセスできる状態に戻すこと、
- データのセキュリティ確保に関する技術的および組織的な対策の効果をテスト、評価すること。

セキュリティの適切なレベルを評価する際、Entrust は処理に伴うリスク、特に処理対象の個人データの予期せぬ、または違法な破壊、紛失、改ざん、不正な公開や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、その第三者は守秘義務のもと、およびデータのセキュリティを確保するために適切な技術的、組織的な対策を行う義務のもと、文書による指示に従って処理を行います。 個人データが、Entrust や正当な第三者以外と共有されることはありません。

何らかの個人データや機密情報が含まれている机や棚は鍵がかけられます。 データ使用者が、モニター/画面に個人データや機密情報が表示されて通行人から見えるような状態にすることはなく、その場を離れる際は必ずコンピューター/タブレットからログオフするか、ロックをかけます。

3.8 個人データのインシデントの報告

次のように、常に個人データのインシデントが発生するおそれがあります：

- 個人データが含まれるモバイル機器やハードコピーのファイルの紛失（例：公共交通利用時にデバイスを置き忘れる）、
- 個人データが含まれるモバイル機器やハードコピーのファイルの盗難（例：車や自宅から盗まれる）、
- 人為的なミス（例：従業員が誤って意図しない人物に個人データが含まれるメールを送信する、個人データを誤って改変または削除する）、
- サイバー攻撃（例：知らない第三者から受信したメールの、ランサムウェアやその他のマルウェアが含まれる添付ファイルを開く）、
- 不正な使用/アクセスを許可（例：Entrust のオフィスやシステムの保護された領域へのアクセスを、権限を持たない第三者に対して許可する）、
- 火災や洪水など、予測不可能な状況、
- 第三者が詐欺を行って Entrust から情報を入手する。

次のようなケースでは、個人データのインシデントが発生した可能性が示唆されます：

- 特にアクティブなユーザーアカウントについて、異常なログインおよび/またはシステムのアクティビティが過剰に発生している場合、
- 異常なリモートアクセスのアクティビティがある場合、

- 偽装されたワイヤレス（Wi-Fi）ネットワークを、Entrust の職場から確認できる、またはアクセスできる場合、
- 装置に異常がある場合、
- Entrust システムにハードウェアまたはソフトウェアのキーロガーが接続、設置されている場合。

個人データのインシデントが発生した、または発生しつつあるということに気付いた、あるいはそれを疑う根拠を持っている従業員は、速やかに Entrust Datacard セキュリティ オペレーティング センター（SOC@entrust.com）およびコンプライアンス ディレクター（privacy@entrust.com）にメールで報告する必要があります。

3.9 個人データのインシデントへの対応計画

個人データのインシデントが実際に発生した、または発生しつつある場合、Entrust はインシデントの影響を最小限に抑えるために素早く対応し、法律によって求められている場合はインシデントの報告を行います。 大抵の場合、対応時に次のようなことを行います：

- インシデントを調査し、性質、原因や、結果として発生し得るダメージ、損害の規模を判断する、
- インシデントが継続または繰り返し発生するのを防止し、データ主体への影響を抑えるために必要な措置を講じる、
- 他の関係者（例：国内のデータ保護当局、影響を受けるデータ主体）に通知する義務があるか判断し、通知を行う。 データ保護当局に通知する義務がある場合は、通常、会社（あらゆる従業員を含む）がインシデントに気付いてから 72 時間以内に報告を行う必要がある、および
- 通知を行う、または行わないという判断について説明する文書を含めて、個人データのインシデントに関する情報と行った対応策についての情報を記録する。

3.10 国際的なデータの転送および第三者への転送

Entrust は GDPR に従い、適切なレベルでデータを保護できる、または Entrust がデータを保護するために適切な措置を講じている、欧州経済地域（以下、「EEA」）外の国に個人データを転送することができます。

EEA 外かつ Entrust グループ内で移転する個人データのセキュリティを適切に確保するために、Entrust グループの各企業（つまり、すべての企業および子会社）は Intra-Group Data Transfer Agreement（グループ内データ転送契約）を結ぶ必要があります。

Entrust を代表して、あるいは 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、Entrust がデータ管理者またはデータ処理者とみなされる場合、EEA 域外に移転する個人データのセキュリティを適切に確保するために、Entrust とデータ処理契約を結ぶ必要

があります。 この契約には、対象の第三者が技術的および組織的な対策を適切に行い、GDPR を遵守し、確実にデータ主体の権利を保護するという文言が含まれます。

次のような場合などに、Entrust は EEA 域外の国に個人データを移転します：

- データ転送に伴って発生し得るリスク（例：国内に同程度の安全策がない）のことを Entrust が通知した後、データ主体が明示的に同意した場合、
- データ主体との契約内容を遂行するため、または契約前にデータ主体の求めで発生する手続きを行うために転送が不可欠である場合、
- データ主体や、データ主体が身体的または法的な理由で同意を行えない場合は別の人物の不可欠な利害を守るために転送が必要である場合、
- 法的主張を確立または弁護するために転送が必要である場合。

EEA 域外にデータを転送する際、Entrust は欧州委員会が定めている標準的契約条項（2001/497/EC, 2004/915/EC および 2010/87/EU）に準拠します。 また、カナダ外に個人データを転送する際は、データ転送契約も必要になります。

3.11 データ主体への通知

個人データの処理について、データ主体に情報を提供することが Entrust に求められています。これに関する情報は、www.entrust.com で公開されている会社のプライバシーに関する声明、および Entrust のイントラネットで入手できる従業員のプライバシーに関する声明に含まれています。 これらの声明には次のような情報が含まれています：

- 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および法的根拠、
- 処理過程で第三者に個人データが開示されるかどうか、
- EEA 域外およびカナダ以外に個人データを転送するかどうか、また転送する場合、どのような対策を講じるのか、
- 個人データを処理する期間、またはそれを判断できない場合、処理期間を判断するうえで会社が使用する基準、
- Entrust が保持する個人データのコピーをデータ主体が入手する方法、
- 申し立てを行う方法を含む、データ主体の権利、
- 法律または契約を遵守するために個人データを処理する必要があり、かつデータ主体がデータの提供を怠った、または処理を拒否した場合に発生し得る結果、
- 該当する場合、自動化された判断プロセスの有無、およびその詳細情報。

Entrust が第三者からデータ主体に関する個人データを受け取った場合、会社は次のような情報もデータ主体に提供します：

- 第三者から受け取った個人データの種類、

- データの取得元についての情報、および公開されている情報元（例：公開されているウェブサイト）かどうか。

3.12 プライバシーを考慮した設計およびデータ保護の影響評価

データ保護法により、新製品の開発段階からデータ保護に配慮することが Entrust に求められています。 この義務を果たすために、Entrust はデータ保護を設計過程に盛り込み、収集する個人データが最小限になるよう、措置を講じる必要があります。

一部のケース（例えば、個人の権利および自由に対して大きなリスクが処理に伴う場合）では、個人データの処理に関連して Entrust が公式にデータ保護影響評価（DPIA）を行わなければならない場合があります。 そのような評価には、アクティビティを実施する目的、Entrust がデータ保護法を遵守する方法、会社が個人のプライバシーに対する潜在的なリスクを緩和する方法を文書化する作業が伴います。 データ保護影響評価が必要だと思う場合は、コンプライアンス ディレクター（privacy@entrust.com）に連絡してください。

3.13 データ主体の権利

データ保護法に基づき、Entrust が個人データを処理する際にデータ主体が次のような権利を持つ場合があります：

- 保持されている自身の個人データについての情報を求める権利、
- データが不正確または不完全であると Entrust が実際に判断した場合に、不正確な個人データを修正する権利、不完全な個人データを完全にする権利、
- 会社が自身の正当な利害を追求するためにデータを処理する場合に、Entrust による個人データの処理に異議を申し立てる権利。 会社の正当な利益がデータ主体のそれを上回る場合、または法的主張を確立または弁護するために Entrust が処理を継続する正当な理由がある場合、Entrust はこの要求を拒否することができる、
- データ主体自身の個人データの廃棄を Entrust に求める権利。 処理を行うに至った目的のために個人データがまだ必要であり、Entrust が処理を継続する正当な根拠がある場合、会社はこの要求を拒否することがあります、
- 保管する個人データの処理を制限するよう、Entrust に求める権利。 個人データの正確さが疑われ、未検証のままになっている場合にのみ、このリクエストを行うことができます。つまり Entrust が個人データを必要としなくなったものの、データ主体が法的主張を確立または弁護するためにそれを必要としている場合、データ主体が個人データの処理を拒絶した場合、Entrust が自身の正当な利害がデータ主体の利害よりも優先されるかどうかを判断している、または処理が違法であるかを判断している場合です。

データ主体がこれらの権利を行使し、かつ Entrust が対象の個人データをすでに第三者に開示している場合、会社は第三者の側でもデータ主体の希望に応えられるよう最善を尽くします。

3.14 データ主体によるアクセス要求

データ主体はにある Data Subject Access Request（DSAR：データ主体によるアクセスのリクエスト）を提出することで、Entrust が保持している自身の個人データに関する情報を求めることができます。 他の従業員が直接（口頭または文書で）リクエストを受け取った場合は、リクエストの詳細情報を速やかに privacy@entrust.com に転送してください。

3.15 トレーニング

Entrust は従業員および臨時社員にトレーニングを提供し、データ保護に伴う責任について学べるようにしています。 入社時、およびその後定期的にこのトレーニングを行っています。

3.16 データ保護責任者

Entrust の GDPR 担当は、Anjali Doherty、上級 法律顧問です（英国）。 Entrust Datacard Deutschland GmbH が指名しているデータ保護責任者は、Kill & Wolff GmbH の法律事務所です。 Entrust Datacard Corporation は指名されたデータ保護責任者いません。 データプライバシーのコンプライアンスプログラムに対する違反に対応するのは、米国ミネソタ州シャクスガンにある Entrust の本社勤務のコンプライアンスディレクター、Jenny Carmichael です。

4. コンプライアンス

このポリシーを遵守することが、すべての従業員および臨時社員に求められています。 さらに、すべてのビジネスユニットが現地の標準および手順を適切に準備し、このポリシーおよび対象の管轄地域におけるデータ保護の規制を遵守しなければなりません。 このポリシーへの違反行為は厳しく処理され、最悪の場合の解雇を含む懲戒処分につながるおそれがあります。このポリシーは任意の時点で更新または改定される場合があります。

5. 例外

このポリシーに対する例外はありません。

6. 所有者およびレビュー

このポリシーは、総合委員会/チーフコンプライアンスオフィサーが所有しています。 毎年、このポリシーのレビューを行います。 このドキュメントに対する変更は、ISMS ドキュメントおよび記録管理標準に則った形で行います。

6.1 連絡先情報

このポリシーに関する疑問や、個人データの扱いが不満である場合は、コンプライアンス ディレクター（privacy@entrust.com）に連絡してください。