

原文: [CareAR-Takes-Security-and-Privacy-Seriously](#)

CareAR のセキュリティとプライバシーに関する取り組み

CareAR ではお客様の成功こそが当社の成功であると認識しています。成功は信頼の上に成り立つものです。そのため、当社は個人情報保護とプライバシーへの取り組みについて透明性を保つことが重要だと考えています。

EU、スイス、英国でのサービス提供におけるプライバシーとデータ保護に関する CareAR の取り組みについて

一般データ保護規則

欧州連合の一般データ保護規則（GDPR）は 2018 年 5 月 25 日に発効されました。この規制は EU 市民に対して個人データおよびプライバシーの保護を強化するもので、自己の個人データをより確実に制御するための EU の試みです。

CareAR は GDPR 施行後に設立されたため、最初からプライバシー保護を念頭に置いたサービス設計となっているのが強みです。個人情報の保護は信頼の根幹をなすもので、CareAR のユーザー様は安心して当社のサービスをご選択いただけます。本文書ではプライバシーおよびデータ保護に対する当社のコミットメントの概要を記載しています。当社の取り組みに関する正式かつ詳しいご説明は、当社ウェブサイト（<https://carear.com/privacy-policy/>）でご覧いただけます。

当社が収集するもの

当社は個人データを含む以下の情報を収集し、処理します。当社のサービスおよびそれに供するモバイルアプリを利用するためにそれらが必要であるためです。

- コンタクト情報
 - 氏名、電子メールアドレス、電話番号（任意）
- アプリ使用時に収集される端末データ
 - 例えば、デバイスのモデル識別子、オペレーティングシステムの識別、ネットワーク信号、IP アドレスを含むネットワーク接続、サービスの利用日時、サービスのパフォーマンス、アプリで使用している機能、GPS 座標（任意）などです。
- アプリの動作に必要なアクセス
 - ユーザーのモバイル端末の通知、カメラ、マイクへのアクセス（上記の機能の使用状況に関する情報を収集します）
- 音声および映像
 - ユーザーが他のユーザーとサービスコールを行う場合、インターネットを介して音声や映像を伝送しています。当社は通話内容の閲覧や傍聴はしていません。また配信後の音声や映像の保存も行っていない。
 - コール中にアプリを使って撮影した写真

個人データの送信先と保護方法

CareAR Assist バージョン 21.04 以降では、管理ポータルでメディア（映像および音声）の送信可能地域を以下のように設定することができます。

- グローバル
- アジア
- 中国

- ヨーロッパ
- インド
- 日本
- 北アメリカ

例えば、映像や音声をヨーロッパ圏内に限定したい場合、この設定を使用すると、音声や映像がヨーロッパ圏内にのみ送信されるようジオフェンスを有効化できます。

当社は個人データを処理する際に、適切な物理的、技術的、管理的および組織的措置を適用し、関係する個人データの種類に応じた機密性とリスクに見合った取り扱いをしています。EUで収集された個人データは、保存時に暗号化されます。個人データは安全に当社のデータベースサーバーへ伝送されます。現在、当該サーバーは米国のGoogle Cloud Platform (GCP) によってホストされています。GCPのクラウドプラットフォームのセキュリティについての説明は、こちら (<https://cloud.google.com/security>) をご覧ください。

データ主権

データ主権では物理的な地理上の範囲内でユーザーおよび使用データを物理的に保存することについて論じられています。

CareAR Assist 22.02.002 は、データ主権をアーキテクチャによりサポートしています。具体的には、顧客データの恒常的な保存先として以下の地域の1つが指定される場合があります。これらのデータには、ユーザーのメールアドレスを除く、ユーザーおよび利用情報に関連する個人を特定できる情報 (PII) を含みません。

- 米国
- ドイツおよびベルギー
- カナダ

ユーザーマッピングおよび認証

データ主権の観点から、ユーザーの初回ログイン時に、*位置情報データベース*を照会して、ユーザーがどの地域に割り当てられるかを決定します。位置情報データベースへの入力項目は、1) ユーザーのメールアドレス、2) ユーザーのテナントが属する地域です。不明な場合、デフォルトの場所は米国となります。

テナントの地域が決定されると、その後のユーザー（ログイン中）のやり取りは、その地域で実行されるサービスロジックに管理されることとなります。現在、ユーザーの認証は*グローバル認証サービス*を使用して実行されています。

カナダまたはドイツでテナントを導入することをご希望のお客様は、CareAR テクニカルサポートオペレーションチームにお問い合わせください。詳しくは、[CareAR Assost22.02.002 のリリースノート](#)をご覧ください。

その他の取り組み-コンプライアンス、ポリシー、プロセス

CareAR は当初から、GDPR の精神と要件の両方を満たすために真摯に取り組んできました。ここでは、コンプライアンスのために取り組んでいることを、さらにご紹介します。

まず、当社では個人データの保護とプライバシーに対する取り組みについて透明性を確保しています。当社のプライバシーポリシーでは、個人データを保存、保護、使用する方法を、ユーザーが確実に管理できるようにするため、当社が実行する手順を明らかにしています。当社のポリシーは <https://carear.com/privacy-policy/> に掲載されており、最新の改訂日と最新の変更点の概要が表示されています。そこでは、当社がどのような個人データを収集するのか、その収集目的、個人データを安全に取り扱い保管するための取り組み、および GDPR の下で個人が自己の個人データに関する権利を行使する方法について説明されています。

CareAR では、当社ウェブサイトのプライバシーページ（上記リンク）において、データ主体が権利を行使するためのプロセスを定めています。データ主体が自己の個人データのコピーを要求する場合やその削除または処理の制限を要求する場

合、さらには個人データの使用に対する同意を撤回する場合など、プライバシー関連の事柄について当社と連絡を取るためのリンクを提供しています。法の要求として、いかなるデータ主体の要求であっても、当社がそれを処理する前に、データ主体は合理的な範囲で自己認証を行い、当該個人データが本人に帰属するということを保証しなければなりません。当社の顧客契約が要求する範囲において、データ主体を特定の顧客と関連付けることが可能な場合、当社は顧客と協議し、データ主体の要求に応じる可能性について確認します。

また、当社の復処理者のリストを、<http://carear.com/gdpr-subprocessors> で公開しており、当社は GDPR の要件を満たす合意事項を各契約に含めています。このリストは常時更新され、新規の復処理者を本番環境に導入する際には、速やかに更新されます。

さらに、ゼロックスの一員として、ゼロックスのグローバル・チーフ・プライバシー・オフィサーおよび情報セキュリティチームと協議することで、データ保護とプライバシーへの取り組みを強化し、当社が取り扱う個人データの内部ポリシー、プロセス、保護を確実なものにしています。さらに、当社では全従業員が個人情報取り扱い方法や保護する方法を確実に理解するよう、情報セキュリティ研修を毎年実施しています。また、従業員が潜在的なセキュリティ・インシデントを報告するための方法が文書化されています。同時に、報復を恐れることなく匿名で不正行為を報告するための内部告発ホットラインも用意されています。

プライバシーとデータ保護に対する当社の継続的なコミットメント

CareAR では、このプロセスが単に GDPR 規制を遵守して終わるべきものではないと考えています。当社は当社が収集し処理する個人データの保護を継続的に改善することをお約束します。