Acronis

GDPR
（EU一般データ保護規則）
よくある質問（FAQ）

FAQ

Q: GDPRとは何ですか？

A: 欧州連合（EU）一般データ保護規則（GDPR）はEU居住者が所有するプライベートデータの保護を強化するEUの新しい法律です。この規則は、EU各国で施行されているさまざまなデータプライバシー法を統一された法律で置き換え、EU全加盟国が直接執行するものです。

Q: GDPRはいつ施行されますか？

A: 2018年5月25日です。

Q: GDPRはEUに拠点を置く企業にだけ適用されるのですか？

A: このよくある誤解に対する答えは「いいえ」です。EUに顧客を持ち、EU居住者の個人データを取得したり、取り扱ったりするいかなる企業もGDPRを遵守する必要があります。

Q: GDPRにおける「個人データ」とは何を指しますか？

A: 「個人データ」とは個人を特定できるあらゆる情報を意味します。これは個人を識別可能な情報の歴史的定義の範疇を大きく超えるもので、個人名、電子メールアドレス、ソーシャルメディアの投稿、身体的・生理的・遺伝子的情報、医療情報、所在地、銀行の詳細情報、IPアドレス、Cookieおよび文化的アイデンティティも含みます。

Q: GDPRは実際、何を規制するのですか？

A: GDPRは、EU居住者が所有するすべての個人データの収集、保存、転送、使用―これらはまとめて処理といいます―を規制します。例えば、ブラウザのクッキーを使用してユーザーの所在地や活動の追跡を行うなど、EU居住者の個人データを処理するすべての組織は、仮に処理組織が物理的にEUに存在しない場合でも、法律の対象となります。

本規制は「コントローラー（管理者）」と「プロセッサー（処理者）」を個人データの取り扱い業者として区別します。個人データの取り扱いとその理由を決定する組織はコントローラーです。コントローラーが個人データのに関して契約を結ぶサードパーティー、例えばクラウドストレージサービスプロバイダーはプロセッサーです。

Q: GDPRはプライバシー権にどのような影響を及ぼしますか？

A: GDPRはEU居住者のプライバシー権を大幅に拡張し、それを保護するために個人データを扱う企業、機関、個人に重要な義務を課します。個人データのプロセッサーが尊重しなければならない新要件には、以下が含まれます。

- **データ主体の権利:** EU居住者は、プロセッサーに対してデータのコピーの提供、間違いの修正、求めに応じて完全に削除することなどを依頼でき、自らの個人データにより強い管理権を持ちます。
- **遵守証明:** プロセッサーは適切なデータセキュリティ方針と手続きを導入し、データ処理活動に関する詳細な記録を保持する必要があります。
- **セキュリティ違反の通知:** データ侵害が発生した場合、プロセッサーは地域のGDPR監督機関に報告し、重大な違反については影響を受けるデータ主体にも報告する必要があります。
- **非遵守に対する罰金:** GDPR規制当局は遵守を怠った組織に違反の深刻さと発生した損害の大きさに基づいて多額の罰金を科す可能性があります。

Q: GDPRでは個人データをEU内に留めることが求められますか？

A: 必ずしもそうではありませんが、GDPRを遵守しながらEU外に個人データを移動する（「国境を超えるデータ転送」）ことは、複雑になる可能性があります。いくつかの規則を考えてみましょう。まず、データの受け取り先となる国が、EUが認める「適切な」セキュリティを備えた国リストに含まれる場合、つまり、EUの基準に一致するデータ保護措置が施行されている国である限り、どの国にでもデータを転送できます。一部のケースでは、国全体が「適切」であるとは認められないものの、特定の地域は適切であると認識される場合もあります。2018年の年初では、承認リストには、全EU加盟国、欧州経済地域に含まれる3カ国（アイスランド、リヒテンシュタイン、ノルウェー）、さらにその他の数カ国と地域（アンドラ、アルゼンチン、カナダ、フェロー諸島、ガーンジー島、マン島、イスラエル、ジャージー島、ニュージーランド、スイスおよびウルグアイなど）が含まれます。

また、データ転送は拘束的企業準則（BCR）のEU標準を満たす受取先にも許可されます。これにより一定の企業内法人や、場合によっては、共同経済活動に携わる独立企業のグループへの個人データの転送が許可されます。資格を得るためには、準拠するBCRは適切な監督機関によって承認され、EUの一貫性基準に適合する必要があります。

他のデータ転送先は通常、業界団体またはその代表団体のひとつが策定し、GDPR規制当局が承認する一定の「行動規範」および「証明制度」に適合する場合許可されます。

さらに他のデータ転送は、「特別免除」すなわち標準の規則に対する例外に該当する場合正当なものです。以下に該当するデータ転送がその一例として挙げられます。

- データ主体が関連するリスクについて理解し、これに同意する
- プロセッサーは、契約上の義務を果たす、または法的主張を満たす必要がある
- 公の利益またはデータ主体の重要な利益に適っているとみなされる
- データ主体の権利を妨害しない限り、データコントローラーの「正当な利益」に適っているデータコントローラーはデータ転送の状況を評価し、合理的な手段を用いて個人データを保護する必要があります。

つまり、一般的に企業にとっては、個人データをEU域外またはその承認の最終候補国外に転送しないほうがより単純で、より安全で、より安価となります。費用の若干の増加に備え、個人データを他の場所に転送するよう努め、GDPR監督機関に個人データを保護するために行ってきた手段について証明する準備を行ってください。BCR、行動規範、証明制度および/または特別免除に依拠する場合、必ず信頼できる弁護士に相談して、他の種類のデータ転送を正当化してください。

Q: GDPRはセキュリティ違反対策にどう影響しますか？

A: GDPRでは、コントローラーとプロセッサーの両方がシステムを配置し、潜在的なセキュリティ違反に対して保護、監視、報告を行い、違反の予防、検出、報告および通知を行うために技術、方針、手続きを文書化し、実行するよう求めます。より厳格化された新しい情報開示要件は、偶発または故意を問わず、権限のない当事者が個人データに対してアクセス、転送、改変、または破壊された事案に適用されます。

プライバシー保護の事案は、技術的障害（例えばハードドライブのクラッシュ）、偶発的な人的エラー（例えばITスタッフが偶発的にユーザーファイルを削除または破損した場合）、または故意で悪意を伴う違反（例えば、個人データを暗号化し、そのブロック解除に金銭を要求するサイバー犯罪者によるランサムウェア攻撃）などによって起こる可能性があります。

最も基本的な条件下で、コントローラーとプロセッサーは個人データに影響を及ぼすセキュリティ事案を特定し、それを監督機関に事案発生から72時間以内に報告し、深刻な個人データの損害、盗難または損失があった場合には、影響を受けるデータ主体にも迅速に通知する必要があります。

Q: コントローラーはどういった新しいユーザー権利をサポートする必要がありますか？

A: GDPRによってデータ主体は、コントローラーによる自分の個人データの使用に対しより強いコントロールを持ち、より明確に把握できるようになります。コントローラーは、求めに応じて、個人データのどの要素を取得したのかをユーザーに知らせ（無償で）、それを容易にアクセスできるフォーマットで提供し、ユーザーが特定した誤りを修正し、依頼に応じて個人データを削除（いわゆる「忘れられる権利」）する義務を負います。

Q: データ保護責任者とは何ですか。また、コントローラーとプロセッサーにはデータ保護責任者が必要ですか？

A: データ保護責任者（DPO）は、従業員またはコンサルタントであり、多くのコントローラーとプロセッサーがGDPR遵守状況を監視する上で主要な責任を負う担当者として指定する必要があります。公共機関はより高い基準に従います。ほとんどの公共機関がDPOを任命する必要があります。民間組織は、データ主体の人種、民族的起源、政治的意見、宗教または思想的信条、遺伝子学的またはバイオメトリックデータ、および/または犯罪歴などを示す大量の個人データを処理する場合にのみDPOを任命する必要があります。

DPOはデータ保護法やベストプラクティスの知識を持ち、訓練を受けたコンプライアンスの専門家であるべきです。その職務は会社のコントローラー、プロセッサーおよび従業員にGDPR下での義務を伝え、遵守を監視し、監督機関との連絡役としての役割を果たすことです。

Q: コントローラーまたはプロセッサーもしくはその両方がGDPR規制を遵守しなかった場合はどうなりますか？

A: GDPR非遵守の罰金は少額ではありません。組織が記録文書を保管していない、または遵守目標を満たすために適切な技術的、組織的手段を講じていないと認められた場合には、管轄の監督機関は、1千万ユーロまたは年間収益の2%のいずれか大きい方を罰金として科す可能性があります。重大なデータ侵害や個人データを盗難、改変または削除から保護しなかった場合などのより深刻な犯罪に対しては、罰金が2千万ユーロまたは年間グローバル収益の4%のいずれか大きいほうにまで上昇します。

罰金はコントローラーおよびプロセッサーの両方に適用される可能性があることに注意してください。監督機関は、GDPRを遵守するためにコントローラーとプロセッサーが取った手順に基づいて違反を評価し、それぞれの責任に比例して罰金を配分することができます。

これらの深刻な罰金に加えて、GDPR遵守義務を故意に無視したり、過小評価したりする会社は、企業の評判を永続的に傷つけ、個人データ違反が発生した場合に、「物質的または非物質的」な損害に対して民間人から訴訟を受けるなどの問題に直面します。上記の罰金と制裁は、サードパーティープロセッサーが他の会社のために個人データを取り扱う場合にも等しく適用されます。データ侵害が近年飛躍的に増加していることを考えてみましょう。

例えば、ランサムウェア攻撃を使った違法ビジネスが2015年は年間80万USドルだったのが、2018年には80～100億USドルに到達すると予想されています。データ侵害に対する報告義務違反だけでも大きな問題となる可能性があります。

Q: GDPR遵守を達成する責務は大きすぎるようです。どこから開始すればいいですか？

A: データ保護ソリューションのプロバイダーとして、Acronisはデータストレージとバックアップインフラのアップグレードを重視することがGDPR遵守への最初の一歩だと確信しています。データが正確にどこに保管されているのかを特定でき、ランサムウェアなどの攻撃を予防し、また転送中、保管時を問わず強力な暗号化でデータを保護することが、GDPR遵守の取り組み姿勢として、具体的で好影響をもたらす基礎になります。

しかし、GDPRの課題に取組む方法を決定する場合には、当社に依拠すべきではなく、必ず適切な弁護士および専門家の助言も得るようにしてください。

本FAQは情報提供のみを目的として作成されています。本FAQは、法的助言として意図されているものではなく、または法的助言として信頼、解釈されるべきものではありません。法的助言またはその他の専門的助言を伴わずに、本FAQの内容に基づいて行動を起こす、または行動を控えるべきではありません。

Acronis

追加情報はこちらをご参照ください：https://www.acronis.com/ja-jp/gdpr/