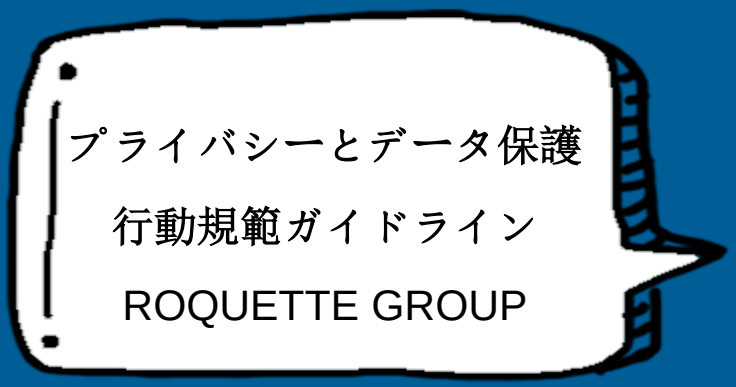
PUBLIC

ROQUETTE
Offering the best of nature™

Privacy & Data Protection

日々のプライバシーとデータ保護への取り組み



法務＆コンプライアンス

Roquetteのコンプライアンスに関する主な課題

Roquette におけるコンプライアンスの適用範囲とその管理は、経営陣のリーダーシップのもと、グループの「法務・コンプライアンス」部門の重要な一部となっており、コンプライアンス・オフィスとして知られています。

コンプライアンス・オフィスは、Roquette 行動規範 とその更新および実施に関する権限を有しています。

また、主に以下の 3 つの分野をカバーしています：

- 財務上のセキュリティ
- 職業倫理
- プライバシーとデータの保護

そのため、コンプライアンス・プログラムが策定され、当社の事業が法的にも財務的にも問題のないものであることを保証するために、現在も継続して更新されています。

コンプライアンスの役割とは？

コンプライアンスの役割は、**倫理的価値観**を浸透させ、**法的要件や基準、適正な慣行**に従って対策を実施することです。

当プログラムは、Roquette に適用される規則の遵守を保証する手順の実施を促進するものです。

「Authenticity（真実性）」「Excellence（卓越性）」「Forward-looking（未来志向）」「Well-being（健康と幸福）」という4つの価値観は、私たちが日々行動するための揺るぎない基盤となっています。

当社のデータ保護は、人とビジネスを中心とした戦略です

プライバシーとデータ保護の原則は、当社の行動規範に定められた基準の一部です。

倫理はグループの重要な価値観として語られることが多くなっており、データ倫理はその重要な一部です。

ご挨拶

プライバシーとデータ保護の原則は、当社の行動規範に定められた基準の一部です。

すべての従業員、およびRoquetteが関係を持つ第三者には、プライバシーを守る権利があります。そのため、Roquetteはお客様の個人情報の保護に努めています。

個人情報とは、直接または間接的に個人を識別できる情報（氏名、生年月日、社会保障番号、写真、電子メールアドレス、コンピュータIDなど）を指します。

個人情報の保護は、プライバシーを確保する基本的な権利です。

個人情報の保護は、各個人がこのデータの収集、処理、使用、配布を管理する権利を保証します。

個人データは、特定の、明示的かつ合法的な目的のために、公正な方法で使用され、処理の実行に必要な期間のみ保管されなければなりません。

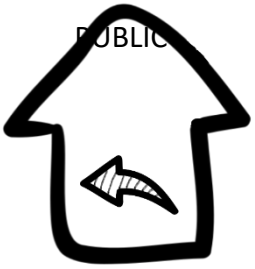
欧州では、2018年5月25日に施行された一般データ保護規則（GDPR）により、個人データの取り扱いが定義されました。

プライバシーおよび個人情報に関する法律は国によって異なるため、またRoquetteでは国際的に事業を展開していることから、当グループでは個人情報保護に関するグループポリシーを採用しています。本ポリシーは、全世界のグループ従業員に適用されます。

本ガイドラインは、個人データ保護原則および当社ポリシーの要求事項を遵守するために、当社の日常業務で採用すべき「行動規範」について説明するものです。

Jennifer GODIN、データ保護責任者

Déléguée à la protection des données



目次

目的

プライバシーおよびデータ保護ポリシーとは？

Roquette Group は、自社のイメージ、利益、データ保護に関する適用法および規制に沿って、プライバシーおよびデータ保護の問題に最適に対処するために、プライバシーおよびデータ保護ポリシー（以下「ポリシー」）を確立しています。

本ポリシーは、個人情報の保護に関する原則と要件を定義し、プライバシーとデータ保護の観点から、すべての従業員、マネージャー、取締役、および Roquette のために行動する第三者が遵守すべき規則を示しています。

本個人情報保護方針の原則と規則は、3 つのレベルの文書プラットフォームで詳細に説明されています。

- マネジメントのコミットメント：行動規範
- 社内規定：個人情報保護ハンドブックと規定。
- データ保護管理システム（DPMS）の文書化：手順、ガイドライン、方法論、学習など

すべての文書は、データ保護に関する法的要件および規制要件に準拠しています。

プライバシーとデータ保護に関する行動規範とは？

プライバシー＆データ保護ガイド（以下「ガイド」といいます）は、当社のプライバシー＆データ保護方針の実施および遵守に役立つものです。

この規程では、当社のグループ指令およびデータ保護に関して当社に適用される法律および規制の要件に準拠する規則とベストプラクティスを簡潔に提示しています。

これは、行動規範に基づくテーマに分かれており、「プライバシーとデータ保護」はコンプライアンスのテーマの 1 つです。

説明

プライバシーとデータ保護に関する行動指針は誰に適用されますか？

行動規範は、世界中のすべての事業体にとって共通の基盤となるものです。適用対象：

- 全従業員、取締役およびマネージャー（以下総称して「従業員」と呼びます）
- Roquette の代わりに業務を行う第三者：
  - 契約業者（コンサルタント、フリーランサー、臨時スタッフを含む）
  - 研修員
  - Roquette 以外の事業体からの出向者
  - 非正規労働者
  - その他の代表代理人
  - Roquette が雇用または雇う第三者。

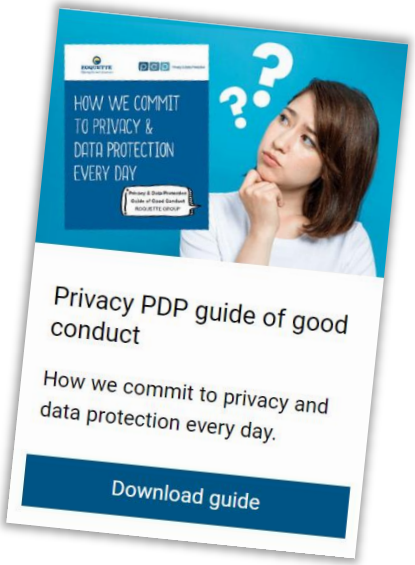
プライバシーとデータ保護に関する行動規範はどこで入手できますか？

Roquette のために行動するすべての従業員と第三者は、当社の文書、特に本ガイドに含まれるプライバシーとデータ保護の原則を理解し、尊重する必要があります。

このガイドは以下についてご覧いただけます。

https://www.roquette.com/data-protection.

このガイドは、プライバシーとデータ保護の原則（国際基準と GDPR の具体的な要件によって定義）に関する e ラーニングコースを備えたツールキットとともに、専用のコミュニケーションの一環として提供されます。



責務

誰が行動規範の履行に責任を持つのですか?

データ・プライバシーは、私たちの組織内のすべての人に関係するものであり、私たちの責任です。

私たちは全員、コンプライアンス・オフィス・チームおよびデータ保護ネットワークが提供する DPMS 文書に記載されている行動規範を遵守する責任があります。本ガイドは、この実施を後押しし、コンプライアンスレベルを向上させるものです。

どうすれば私たちは正しい決断を下していると判断できるのでしょうか?

この行動規範は、私たちの社会生活において、プライバシーに関する疑問が生じる可能性のあるほとんどの状況に対処するためのものです。ただし、現在の文書は私たちが職業的活動の実施において直面するすべての個別状況を予見することはできません。

何らかの折に、とるべき行動について疑問がある場合は、以下の質問に自分で答える必要があります:

- これは法律に従っていますか?
- これはあなたや会社に良い影響を与えますか?
- 友人、家族、同僚にこのことを話しますか?
- このことが公にされても、私は安心できますか?

これらの質問への答えのいずれかが「いいえ」であれば、これ以上先に進むべきではありません。疑問がある場合は、グループデータ保護責任者またはその他の関連する連絡先（「質問または懸念の提起」のセクションの連絡先を参照）に相談してください。

プライバシーとデータ保護の原則に従わない場合はどうなりますか?

行動規範を遵守しない場合は、当社に悪影響を及ぼす恐れがあります。その結果は、企業にとっても、関与した個人にとっても、非常に深刻なものとなる可能性があります（懲戒処分、罰金、懲役、評判の悪化など）。

実際に規範への違反があった場合、またはその疑いがある場合の報告はすべて、重く受け止められます。私たちは、迅速かつ公正に、法的要件に従って調査を実施します。

違反の性質に応じて、現地の会社の規則や法律に従って懲戒処分を受ける場合があります。

すべての従業員は、あらゆる調査に全面的に協力する必要があります。Roquette は、すべての関係者の守秘義務を守ります。

質問または懸念事項を提起する

従業員、Roquette のために活動する第三者およびその他の利害関係者は、会社に対する危害を防止および軽減するのに役立つ疑問や懸念を、Roquette に提起するよう奨励されます。

提起できるのはどのような懸念ですか?

プライバシーおよびデータ保護原則、社内規定、または適用法に違反する可能性がある場合、または実際に違反した場合、あらゆる質問を提起することができます。

あなたが連絡すべき相手とは?

データ漏えいが発生した場合は、 dpo@Roquette.com のデータ保護責任者に連絡　するか、プライバシー警告ウェブフォーム を使用して問題を報告してください。

コンプライアンス違反の可能性を報告する必要がある場合は、通常の連絡先に連絡するか、Speakup©デバイスを通じて問題を報告することができます。このデバイスを通じて受信されるすべての警告は、関連する法律や規制を遵守し、機密情報として取り扱われます。

Roquette では、プライバシーおよびデータ保護原則または適法に違反する可能性がある、または実際に違反があった場合、誠意をもって報告した従業員または第三者に対するいかなる形の報復行為にも厳しく対処します。

したがって、職務上の警告の発行者が自身を特定しなければならない場合、事実を告発したことに対する報復、差別、または懲戒処分のリスクを回避するために、組織は自身の身元を機密として処理する必要があります。

法令の遵守

グループの各組織にいる各自が勤務する国のデータ保護に関して施行されている法令を遵守するよう期待されています。

地域の法律がポリシーおよびガイドより厳格な場合は、その法律が優先されます。

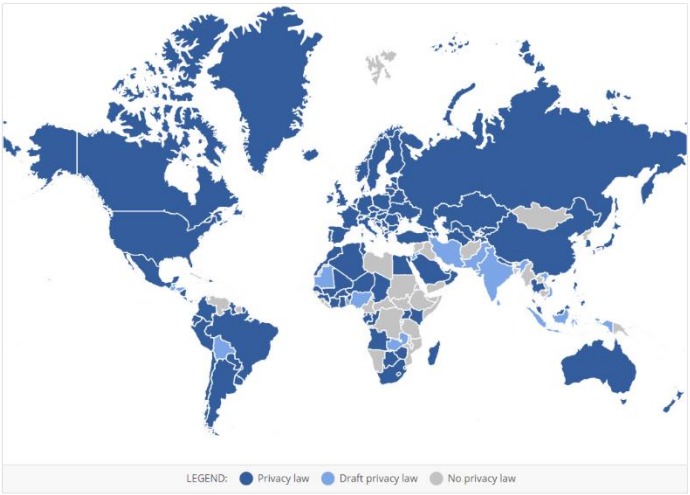
そうでない場合（現地の法律がない、または制限の少ない法律）、法律で許可されている範囲で当社の内部の行動規範が優先されます。

私たちの考え：

- すべての新しい現地法や該当する規制を、できる限り速やかに実施する必要があります。
- 法令違反は、関与した人と会社の両方が民事的および刑事的制裁の対象となる場合があることを、認識する必要があります。
- 個人情報の処理に関連する自然人の保護は、基本的な権利です。
- 個人データの処理に関して自然人を保護する原則および規則は、国籍または居住地にかかわらず、基本的な権利と自由、特に個人データの保護に対する権利を尊重する必要があります。
- 個人情報の保護に対する権利は絶対的な権利ではなく、社会に関連して考慮され、比例性の原則に従って他の基本的権利とバランスを取る必要があります。

特定のデータ保護法を採択している、またはデータ保護局を設置している国は？

概要については以下を参照：
https://www.cnil.fr/en/data-protection-around-the-world



私たちの責任：

- いかなる状況においても、当社は、データ対象者の国で適用されるデータ保護に関するすべての法律および規制、ならびに当社の各拠点で施行されているすべての規則を遵守しなければなりません。

- 当社の業務活動の一環として、データ保護に関する適用法および規制に違反すると思われる行動を報告する必要があります（例：：GDPR）、弊社のデータ保護責任者（dpo@Roquette.com）および機密の Roquette 警告デバイス：Speakup©

- 当社は、他の法律や規制の遵守を容易にしながら、状況に適切かつ比例した個人情報保護対策を講じる必要があります。反対に、グループに適用される法律および規制を遵守するための当社の行動は、個人データの保護に関する規則および良好な実践に準拠していなければなりません（例：贈収賄防止および腐敗防止コンプライアンスプログラムでは、内部通報者の機密性と個人データの保護対策を通じて内部通報者の保護を確保する必要があります）。

一般データ保護規則（GDPR）の対象ですか？

あなたは 、**処理**者〔1〕または**管理**者〔2〕として GDPR の対象になります。

- お客様が欧州連合に居住している場合、または
- お客様が欧州連合に所在していない場合、「処理活動が以下に関連する場合」：
  - EU 域内のデータ主体に対する商品またはサービスの提供
  - または EU 域内のデータ主体の行動の監視

公式文書： GDPR 第 3 条 地域の適用範囲

〔1〕&〔2〕：38 ページの定義を参照してください

データ保護の原則

個人データは以下に準拠します：

- 安全を確保。
- 正確で最新。
- 公正かつ合法的に処理される。
- 限定された目的のために処理される。
- 適切で、関連性があり、過剰ではない。
- 一定の期間にわたって保持される。
- データ主体の権利に従って処理される。
- 他の国に移転する場合は、適切な法的措置によって保護される。

あなたの権利：

適用される法律および規則に従い、ユーザーは、正当な理由によるデータへのアクセス、修正、およびデータ処理に反対する権利、正当な理由によるデータ消去の権利、データポータビリティの権利、およびデータ処理を制限する権利を有します。

これらの権利を行使するには、以下のフォームに記入してください。Roquette.com/ データ保護 。

ご質問がある場合は、**データ保護オフィサー**（dpo@Roquette.com）にお問い合わせください。

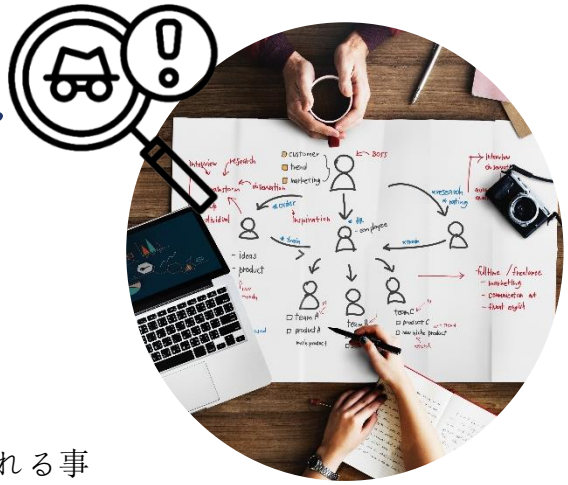
私たちの責任:

私たちがすべきこと:

- 個人情報保護に関する現地の法律およびグループポリシーの規則に従うこと。
- データ保護責任者に新しい処理または変更を通知する。
- 特定の正当で必要な目的以外は、個人情報の収集、使用、開示、保存を行わないこと。
- 個人がデータの収集について通知されていることを確認する。
- これらのデータを収集、処理、使用、通信、保存または転送する際に保護してください。
- 処理されたデータの安全性と機密性を確保します。
- データは処理に必要な期間のみ保持し、適用される法律に従ってください。
- 個人データに関連するセキュリティインシデントが発生した場合は、データ保護責任者に連絡してください。

私たちは従業員を教育し、社内プロセスを改善します。

プライバシーに関するリスク



プライバシーリスクとは？

リスクとは想定されるシナリオのことで危惧される事象とそれを引き起こすすべてのリスクを記述したものです。具体的には次のとおりです。

- どのようにリスク源 （例：：競合他社から賄賂を受けた従業員）
- サポート資産の脆弱性を悪用する可能性がある（例：データの操作を可能にするファイル管理システム）
- 脅威のコンテキスト（例：電子メールの送信による誤用）
- リスクのある出来 事が起こることを許す（例：個人データへの不正アクセス）
- 個人データ （例：カスタマーファイル）
- データ主体のプライバシーに影響を与える（例：望ましくない勧誘、プライバシー侵害、個人的または職業的な問題）。

プライバシーに関する不確実性の影響

重大度はリスクの大きさを表します。主に、既存の、計画された、または追加の管理を考慮して、データ主体に対する潜在的な影響（ **物理的** 、 **物質的、倫理的）** の程度から評価されます。

例：

内部通報者に対して職業上の警告システムが提示する最も重要なリスク：事実を告発したことに対する報復、差別、または懲戒処分のリスク。

私たちの考え：

個人の権利は、処理のリスクレベルにかかわらず完全に適用されます。

ただし、個人情報の処理が個人の基本的権利と自由に与えるリスクのレベルに応じて、データ保護コンプライアンスを調整する必要があります。

GDPR はこの規範にさらなる推進力を与えています。その結果、個人の基本的権利と自由に対するリスクがより低い処理業務は、一般的にコンプライアンス義務がより少なくなる可能性がある一方、「リスクが高い」処理業務は、データ保護影響評価（DPIA）のような追加のコンプライアンス義務が生じます。（1）

私たちの責任：

リスクアセスメントは重要です。GDPR に基づき、リスク評価は組織の説明責任とすべてのデータ処理に基づきます。

当社は、データセキュリティ、セキュリティ、データ侵害通知、プライバシー・バイ・デザイン、正当な利益、目的制限、公正な処理など、高リスク処理の DPIA の一部として、およびその他の多くの GDPR 要件に関連してリスク評価を実施する必要があります。

（1）：58 ページの定義を参照してください。

次の場合のリスク：コンプライアンス違反

データ保護の法律および規制（例： GDPR）を遵守しない法人および自然人リスク制裁とコスト：

刑事上の制裁：

- 懲役
- 法人に対する罰金。

民事上の制裁措置：

- 民事損害賠償。

行政上の制裁措置：

- 正式な通知。
- 警告：
- 命令
- 一時的または恒久的な処理制限。
- 認証の取り消しまたは認証を取り消すための命令。
- データ転送の中断。
- 許可の処理または取り消しを中止する命令。
- 課せられた制裁の公表。
- 事前の正式な通知なしの制裁（緊急性基準）。
- 違反に応じて、行政罰金。

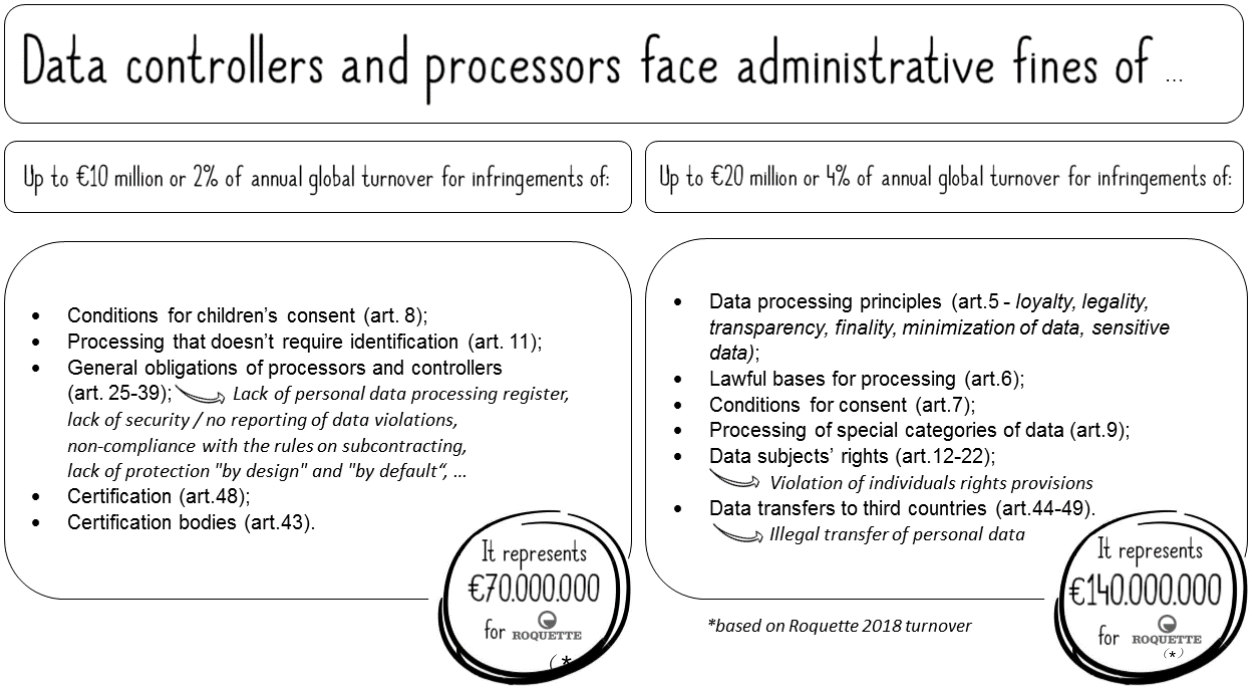
重要なコスト：

- 企業の評判を損なうことによる収益の損失。

GDPR に基づく最高行政上の罰金はいくらですか?

罰金は義務ではなく裁量で課せられます。これらは、ケースバイケースで課せられ、「効果的で、比例し、抑止力のある」ものでなければなりません。

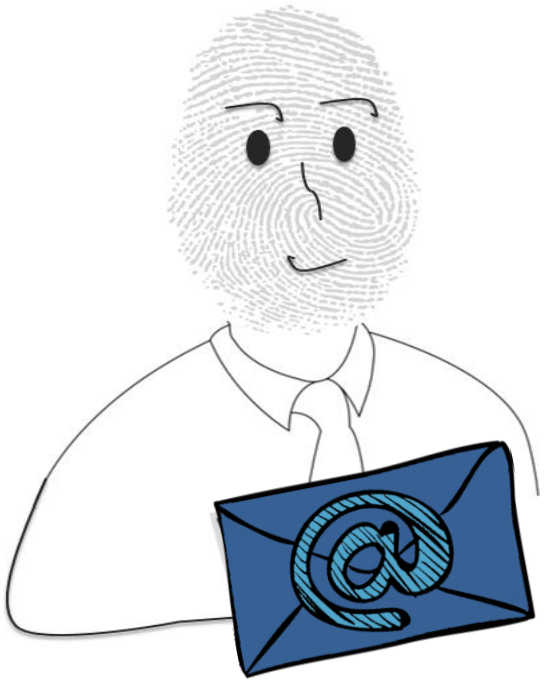
罰金は、組織が違反した規則の特定の条項に基づいています。



刑事上の制裁にはどのようなものがありますか?

フランスの法律の例をいくつかご紹介します。

- 不正、不当、または違法な手段で個人データを収集した行為は、5 年間の懲役と 30 万ユーロの罰金（刑法第 226-18 条）
- 内部通報者の権利と保護を保証するために、汚職防止法（Sapin II）は、通報を妨げるいかなる障害も厳しく罰します。警告に関する機密性は、規制の重要な要素です。したがって、警報の機密要素（内部告発者の身元、被告の身元、警報を裏付けるために提供された情報）の開示は、司法当局に関しては除外して、2 年間の懲役と 3 万ユーロ の罰金の対象となります。



初版

データ対象者との関係における当社の基準

個人情報

データ保護とは、個人に関する個人データの収集と使用を規定する一連の法律、規制、および行動規範です。

「個人情報」とは、識別された、または識別可能な自然人に関するあらゆる情報を意味します。

個人情報とは、個人データの取り扱いを指します。

誰が対象になりますか?

個人情報は、組織内の全員に関連し、全員がその責任を負います。

なぜこれが重要なのですか?

データの誤った取り扱いは、組織、従業員、顧客に深刻な影響を及ぼす可能性があります。

プライバシーの侵害は、金銭的な罰則、悪評、評判の低下、顧客からの信頼の失墜、ビジネスの損失、そして従業員にとっては、クレーム、そしておそらく自分自身の個人データに関するプライバシーの侵害の場合、その他のケースでは懲戒処分の可能性もあります。データを適切に扱うことは、私たち全員の利益となります。

私たちの考え:

- Roquette の全従業員は、個人データの保護に関する役割と責任を認識する必要があります。意識向上の目的は、Roquette 社内のプライバシーと個人データの保護に対する尊重の文化を強化することです。

[DIDPGR001EN - 規則 1]

- 個人情報保護方針の実施に関する従業員のトレーニングを実施する必要があります。

[DIDPGR001EN - 規則 2]

プライバシーに関する声明

それは私たちの責任です！

ビジネスを成功させるためには、顧客と従業員の個人データが必要です。

私たちは、この重要な情報の管理を任されています。

すべての従業員は、適切なデータ保護法を遵守する責任があります。

それが私たちにとっての信頼感です！

信頼感は簡単に失われてしまいます。

お客様と従業員のデータを慎重かつ尊重して取り扱うことは、当社の評判を保護するために不可欠です。

風評被害に対する最大の防御策はあなたです。

それは敬意を表すことです！

お客様と従業員の個人情報の取り扱いに関する選択は、当社への信頼を維持するために遵守する必要があります。

それはあなた次第です！

顧客と従業員の個人データが安全かつ機密に保たれるようにするのは、私たち全員の責任です。

会社を離れて送信または取り扱う必要のある情報には、特に注意を払う必要があります。

私たちは従業員を教育し、社内プロセスを改善します。

- 行動規範 - プライバシーとデータ保護 - 42 - 43 ページ。
- 新入社員の場合：入社時のグローバルオンボーディングでは、データ保護に関するさまざまな情報と e ラーニングが提供されます。
- 従業員を対象：学習は学習プラットフォームにアップロードされます。
- データ保護コーディネーターを対象：ドキュメンテーションは、当社のコミュニティ「データ保護ネットワーク」で共有されています。
- 全員を対象：詳細については、社内ポータル > データ保護をご覧ください。

個人情報の取り扱いについて

個人データの処理とは、収集、記録、整理、構造化、保存、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方法による利用可能化、整列または結合、制限、消去または破壊など、自動化された手段であるか否かを問わず、個人データまたは個人データの集合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。

データ保護（および GDPR）の要件として、個人データの収集には「合法的根拠」が必要であることを認識しておく必要があります。

現地の法律によって、法的根拠が異なる場合があります。

個人データの処理の「法的根拠」は何ですか?

次の質問に明確に答えられる必要があります。

「私の [データ] はどのようにして入手したのですか? なぜ入手が許可されているのですか? 」

具体的には、データ処理の 6 つの法的根拠の少なくとも 1 つを遵守する必要があります。GDPR の下では、以下の場合を除き、データを処理することはできません。

1. 合意がある
2. 契約
3. 法的コンプライアンス
4. 重要な関心事
5. 公開課題
6. 正当な利益

合法性、公正性、透明性

私たちの責任:

個人データの合法的な処理を確実にするために、規則を適用する必要があります。

ルール	OneDoc 基準	GDPR 基準
• データを収集する際は、合法性、公正性、透明性をもって行動する	DIDPGR002EN 規則 1	第 5 条第 1 項 a）
• 関係者の同意が尊重されていることを示す（必要な場合）	DIDPGR002EN 規則 2	第 7 条
• データ収集中に決定された目的を尊重する	DIDPGR002EN 規則 3	第 5 条 1 項 b）
• 紙またはデジタル形式で収集された情報を、厳密に必要なものに制限する	DIDPGR002EN 規則 4	第 5 条 1 項 c）
• データ保持を厳密に必要な範囲に制限する	DIDPGR002EN 規則 5	第 5 条第 1 項 e）
• 個人データを第三国または国際機関に転送するための措置を講じる	DIDPGR002EN 規則 6	第 44 条から第 50 条まで

私たちは従業員を教育し、社内プロセスを改善します。

データ主体の「権利」

情報主体 とは、直接または間接的に、特に、氏名、識別番号、位置情報、オンライン識別子などの識別子、またはその自然人の身体的、生理的、遺伝的、精神的、経済的、文化的、社会的アイデンティティに固有の 1 つまたは複数の要素を参照して特定できる自然人を意味します。

「データ主体」とは何ですか？

これは、特定の個人データが関係する個人を示す技術用語です。

主体者アクセス要求とは何ですか？

現行のデータ保護法が個人に与える主な権利の 1 つは、個人情報にアクセスする権利です。

個人はあなたに「主体者アクセス要求」を送信し、あなたがその人について保有している個人情報について伝え、その情報のコピーを提供することを求めることができます。ほとんどの場合、有効な主体者アクセスリクエストを受領してから 30(*)日以内に回答する必要があります。

（*）：この期間は、適用される法律またはデータ処理の性質によって異なる場合があります。

その他のデータ主体の「権利」は何ですか？

私たちの責任:

私たちは、データ主体の権利を確保するために規則を適用する必要があります。

ルール	OneDoc 基準	GDPR 基準
• 法的通知が義務に準拠していることを確認する	DIDPGR006EN 規則 1	第 12 条
• データ主体がアクセス権を行使することを許可する	DIDPGR006EN 規則 2	第 15 条
• データ主体が訂正権を行使することを許可する	DIDPGR006EN 規則 3	第 16 条
• データ主体がデータポータビリティの権利を行使することを許可する	DIDPGR006EN 規則 4	第 20 条
• データ主体が消去の権利を行使することを許可する（「忘れられる権利」）	DIDPGR006EN 規則 5	第 17 条
• データ主体が処理を制限する権利を行使することを許可する	DIDPGR006EN 規則 6	第 18 条
• 個人データの訂正または削除、または処理の制限に関する通知	DIDPGR006EN 規則 7	第 19 条
• プロフィール作成を含む、自動化された個人の意思決定の管理	DIDPGR006EN 規則 8	第 22 条

私たちは従業員を教育し、社内プロセスを改善します。

個人情報保護に関する方針

個人データが使用されている場合に通知を受ける権利

当社がお客様の個人データを使用する場合、当社は従業員であるお客様、および Roquette と関係があるすべての第三者に通知する必要があります。

以下について詳細な情報を提供する必要があります。

- Roquette がお客様のデータを使用する理由。
- Roquette が使用しているデータの種類。
- お客様のデータが保存される期間。
- お客様の情報に関する権利。
- データの起源。
- Roquette がお客様のデータを第三者に転送する場合の情報。お客様の名前と転送の理由を含みます。
- データが他の管轄区域に転送されるかどうかに関する情報。これには、関係する国とデータの処理方法が含まれます。
- Roquette がプロファイリングでデータを利用している場合（職場でのパフォーマンス、経済状況、健康などを分析または予測するために個人データが使用される自動処理の一種）。
- DPO への連絡方法。
- 懸念がある場合、監督当局に苦情を申し立てる権利。

これは **プライバシー情報** または **プライバシー通知** と呼ばれます。

Roquette がお客様のデータを収集する時点で、お客様にプライバシー情報を提供する必要があります。Roquette が他のソースからお客様のデータを入手した場合、プライバシー情報を提供する必要があります。これは、プライバシー通知の形式で行うことができます。

これは「**情報を受け取る権利**」と呼ばれます。

ルール	OneDoc 基準	GDPR 基準
• 法的通知が義務に準拠していることを確認する	DIDPGR006EN 規則 1	第 12 条

例：

- Roquette ウェブサイトのプライバシー情報はこちらからご覧いただけます：
  https://www.roquette.com/privacy-notice-website

Roquetteは、どのような場合に、その活動を知らせないでもいいですか？

一般的に、当社はお客様にプライバシー情報を提供する必要がありますが、状況によっては提供する必要はありません。以下の場合です。

- プライバシー情報が既に存在し、何も変更されていない。
- 個人情報を提供することが不可能であるか、または提供するには「多大な労力」を要する場合、または
- プライバシー情報を提供すると、お客様のデータの使用が不可能になるか、またはその使用の理由を深刻に損なう可能性がある。

注記：証拠の隠蔽又は破壊を避けるために暫定的措置が必要な場合、そのような情報は、暫定的措置の適用後に提示することができます。

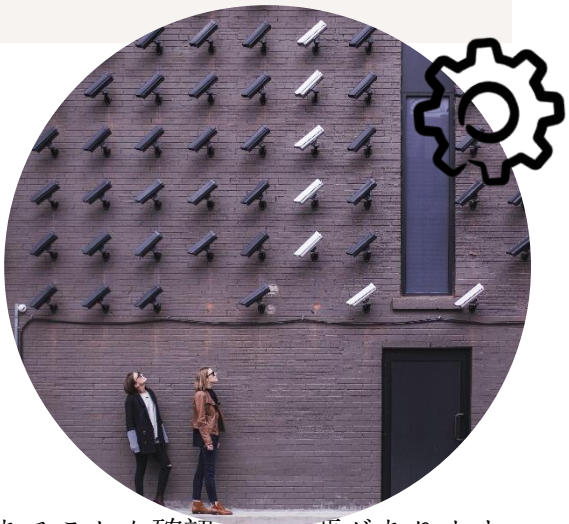
私たちは従業員を教育し、社内プロセスを改善します。

データの最小化

データ最小化の原則とは何ですか?

GDPR - 第 5 条 (1) (c) 項 :

> 「1.個人データは次のとおりです。
>
> （c）処理の目的に関連して、適切かつ関連性があり、必要な範囲に限定される（データの最小化）」



個人データを収集するためにグローバル部門が設計した紙またはデジタルフォームには、処理によって正当化されないデータの収集を避けるため、処理の目的に厳密に必要な情報フィールドのみを含める必要があります。

私たちの責任:

当社は、お客様が処理する個人データが以下のものであることを確認する必要があります。

- 適切であるデータ - 記載された目的を適切に達成するのに十分である
- 関連性 - その目的に合理的な関係がある。
- 必要なものに限定 - その目的のために必要以上の期間は保持できません。

ルール	OneDoc 基準	GDPR 基準
• 紙またはデジタル形式で収集された情報は、厳密に必要なものに制限してください。	DIDPGR002EN 規則 4	第 5 条 1 項 c)

チェックリスト：

- ☑ 当社は、指定された目的のために実際に必要な個人データのみを収集します。
- ☑ 当社は、これらの目的を適切に果たすために十分な個人データを保有しています。
- ☑ 当社は保有するデータを定期的に確認し、不要なデータを削除します。
- ☑ 目的を達成するために必要な個人データの最小量を特定する必要があります。多くの情報を保持すべきですが、それ以上は必要ありません。

説明責任の原則とは、必要な個人データのみを収集・保有するための適切なプロセスがあることを証明できることを意味します。

また、GDPR では、個人は、修正権の下で、あなたの目的に不適切な不完全なデータを補完する権利を有すると述べていることに留意してください。また、消去権（忘れられる権利）に基づき、目的上必要のないデータを削除する権利もあります。

私たちは従業員をトレーニングし、社内プロセスを改善し

データ セキュリティ

サイバーセキュリティ は、関連する情報と資産の適切なレベルの保護を保証しながら、データを共有し、使用できるようにする横断的な活動です。

- **機密性**：情報機密に保たれ、不適切な人物や団体に開示されないようにします。
- **完全性** ：情報と処理方法の正確性と完全性を確保します。
- **可用性**：権限のあるユーザーが必要なときに情報、アプリケーション、サービスに常にアクセスできるようにします。
- **トレーサビリティ**：関連する追跡を維持する能力と、必要に応じて、当社のシステムで何が行われたかの証拠を指します。トレーサビリティには、否認防止やアカウンタビリティといった法的目的もカバーします。

個人情報の資産には以下が含まれます。

- 紙の文書（テキスト、地図、画像など）
- オフィス環境におけるデジタル情報
- モバイル環境におけるデジタル情報
- 職業的なノウハウとスキル（個人が所有するか、口頭で共有）
- 現物（サンプル、模型など）

[DSUG006EN] サイバーセキュリティ指令の管理

偽名化とは、追加情報を使用することなく、個人データを特定のデータ対象者に帰属させることができなくなるような方法で個人データを処理することを意味します。ただし、そのような追加情報は別個に保管され、個人データが特定または識別可能な自然人に帰属しないことを保証する技術的および組織的措置が講じられることが条件となります。

匿名化とは、データ**管理者**(1) が単独で、または他の当事者と協力して、データ対象者を直接的または間接的に識別できなくなるように個人データを不可逆的に変更するプロセスです。

暗号化とは、平文やその他の種類のデータを、読み取り可能な形式から、復号化キーにアクセスできる他の実体によってのみ復号化可能な符号化バージョンに変換する方法です。暗号化は、特にネットワーク経由で転送されるデータをエンドツーエンドで保護するために、データセキュリティを提供する最も重要な方法の 1 つです。

(1):38 ページの定義を参照してください。

私たちの考え：

セキュリティーを維持し、データ保護に関する法令に違反する処理を防止するため、Roquette および当社の業務委託先は、処理に内在するリスクを評価し、**暗号化**または**偽名化**などのリスクを軽減する手段を実施する必要があります。

私たちの責任：

当社は、あらゆる種類の個人データを処理する際にセキュリティ対策を講じる必要がありますが、どのような対策を講じるかは、当社の特定の状況によって異なります。個人データを処理するために使用するシステムとサービスの機密性、完全性、利用可能性を確保する必要があります。

これには、情報セキュリティポリシー、アクセス制御、セキュリティ監視、リカバリ計画などが含まれます。

個人データのライフサイクル全体を通じて、すべての利害関係者が適切なセキュリティ対策を講じる必要があります。

ルール	OneDoc 基準	GDPR 基準
• セキュリティポリシーや指令に定められたセキュリティ対策の適用と見直し	DIDPGROOZEN 規則 1	第 32 条
• 情報セキュリティとデータ保護レビューをプロジェクトに統合する。	DIDPGROOZEN 規則 2	第 32 条
• 設計およびデフォルトによる、セキュリティ、プライバシー、データ保護	DIDPGROOZEN 規則 3	第 25 条
• 下請け業者との、情報セキュリティおよびデータ保護条項の統合	DIDPGROOZEN 規則 4	第 32 条

私たちは従業員をトレーニングし、社内プロセスを改善します。

個人情報分類

機密性の高い個人データや特別なカテゴリーの個人データの処理は、特別な場合を除き禁止されています。

これらの処理には、以下の点に関して保護対策が必要です。

マーキング、アクセス、転送、輸送、コピーおよび印刷、保管およびアーカイ、破壊。

分類は、情報または文書の機密性に適応した保護を 示します。

情報または文書の分類の決定は必須であり、できるだけ早い段階で行う必要があります。

[DISUGR001EN] 情報保護に関する指令

Personal data types	Personal data categories
Common personal data	Civil status, identity, identification data
	Personal life (living habits, marital status, etc. –excluding sensitive or dangerous data)
	Professional life (résumé, education and professional training, awards, etc.)
	Economic and financial information (income, financial situation, tax situation, etc.)
	Connection data (IP addresses, event logs, etc.)
	Location data (travels, GPS data, GSM data, etc.)
Personal data perceived as sensitive	Social security number
	Biometric data
	Bank data
Sensitive personal data in the meaning of [DP-Act]	Philosophical, political, religious and trade-union views, sex life, health data, racial or ethnic origin, data concerning health or sex life
	Offenses, convictions, security measures

私たちの責任:

ルール	OneDoc 基準	GDPR 基準
• 機密データの処理に関する法的枠組みを遵守する	DIDPGROOMEN 規則 1	第 9 条
• 刑事上の有罪判決や犯罪行為に関するデータの処理を禁止する	DIDPGROOMEN 規則 2	第 10 条
• 健康データへのアクセスは認定された専門家に制限する	DIDPGROOMEN 規則 3	第 9 条
• 国民識別番号を一意の識別子として使用することを禁止する	DIDPGROOMEN 規則 4	第 87 条
• 銀行データへのアクセスと使用を制限する	DIDPGROOMEN 規則 5	第 9 条
• 機密データへのアクセスを権限のある人物に制限する	DIDPGROOMEN 規則 6	第 9 条
• 機密データの処理に関与するデータ主体のプライバシーへの影響評価を実施する	DIDPGROOMEN 規則 7	第 35 条
• コメントフィールドの使用を一般情報に制限	DIDPGROOMEN 規則 8	行動規範

実用的なヒントとコツ

分類された情報資産（紙、デジタル、ノウハウ、物理的）の各カテゴリに対して取るべき保護措置の例。

データ保持

グループ、顧客、ビジネスパートナー間の業務と情報交換を非物質化する必要性の増加、ならびに法的要件と規制要件により、Roquette にはデータ保持期間と記録管理ポリシーの観点から多くの義務が課せられています。

Roquette は、当社の活動に基づいて、戦略、財務結果、商業開発またはコミットメントに関連する大量の機密データ、**ならびに顧客、ビジネスパートナー、スタッフメンバーに関連する個人データを取得し、処理します。**

Roquette が当社の活動に関連して送受信した情報は、**個人情報を含む場合を除き、**当社が長期間にわたってアーカイブに保管することを妨げるものは何もないにもかかわらず、最低限の保持期間保持されなければなりません。

管理当局および管轄当局が事後調査を実施できる期間は、保持する情報の性質と関連する法的要件によって異なります。

無期限または無期限の保管期間は禁止されています。

GDPR 第 5 条 1 項 E）

「保管の制限」

個人データは、データ対象者を識別できる形で、個人データの処理目的に必要な期間以内に保存するものとします。

個人情報は、データ対象者の権利および自由を保護するために必要な、適切な技術的および組織的措置を実施することを条件として、公益のための保存目的、科学的または歴史的研究目的、または統計目的のためにのみ処理される限りにおいて、より長期間保存されることがあります。

私たちの責任:

- データ管理者である Roquette は、収集および処理される個人データのカテゴリーごとに、具体的かつ適切な保管期間を定める必要があります。
- 個人データ処理の実施に先立ち、データ保護コーディネーターの支援の下、プロジェクトオーナーはデータ保持期間を当社の登録簿に明記する必要があります。
- 当社は、個人データを処理に必要な期間のみ保存し、適用される法律に従わなければなりません。

ルール	OneDoc 基準	GDPR 基準
• データ保持を厳密に必要な範囲に制限する	DIDPGR002EN 規則 4	第 5 条第 1 項 E)

この点で、グローバル部門、GBU、および地域部門は、会社の情報保持規則を遵守し、関連する手順を運用可能な状態に維持することを約束します。

例:

採用プロセスが終了した時点で、不採用となった候補者については、一定期間（2 年間）「採用候補者プール」に残すことに同意しない限り、情報を削除しなければなりません。

私たちは従業員をトレーニングし、社内プロセスを改善します

2 関連会社および下請け業者との関係における当社の基準

処理者および管理者の資格

管理者 とは、自然人または法人、公的機関、代理店、その他の団体で、単独で、または他者と共同で、個人データ処理の目的および手段を決定する者を指します。

共同管理者とは、処理の目的と手段を共同で決定する 2 人以上の管理者を意味します。ただし、これらの取り決めにかかわらず、各管理者は GDPR に基づく管理者のすべての義務を遵守 する責任を負います。

処理者とは、管理者に代わって個人データを処理する自然人または法人、公的機関、機関またはその他の機関　を意味します。

一般データ保護規則の意味における処理者は誰ですか？

（一般データ保護規則第 4 条 - 定義）
非常に多様なサービスプロバイダーは、法的な意味 での処理者としての能力を有しています。処理者の活動は、非常に特定のタスク（電子メール配信の下請け）に関連するか、より一般的で広範なもの（例えば、従業員の給与管理など、別の組織を代表してサービス全体を管理する）である場合があります。

GDPR の対象となるのは特に次のとおりです。

- データにアクセスできる IT サービスプロバイダー（ホスティング、メンテナンスなど）
  ーター、サイバーセキュリティ企業、IT コンサルティング企業（旧 IT エンジニアリング
- クライアントに代わって個人データを処理するマーケティングまたはコミュニケーショ
- より一般的には、別の組織の代理として個人データの処理を伴うサービスを提供する組
- 公的機関または団体もそのようなものとみなすことができます。

個人情報にアクセスしたり、個人情報を処理したりしない限り、ソフトウェア出版社や機器メーカー（時計端末、生体認証機器、医療機器など）は関係ありません。

処理者と管理者の資格認定例:

会社 A は、会社 B と C のクライアントデータファイルを使用してマーケティングレター配信サービスを提供しています。

会社 A は、会社 B および C の代理として、また会社 B および C の指示に従って、レター文書を送付するために必要なクライアントデータを処理する限り、会社 B および C の処理者です。

企業 B と C は、マーケティングレターの配信に関しても、顧客の管理責任者です。

会社 A はまた、雇用するスタッフの管理、および会社 B と C を含む顧客の管理に関する管理者でもあります。

公式文書 :

- 管理者および処理者の定義に関する一般データ保護規則第 4 条
- 管理者に関する一般データ保護規則（GDPR）第 28.10 条

私たちは従業員を教育し、社内プロセスを改善します。

個人情報保護に関する条項

契約はいつ必要で、なぜ重要なのですか?

管理者として、当社が個人データを処理するために処理業者を使用する場合、当事者間に書面による契約が必要です。
契約は、両当事者が当社の責任と義務を理解するために重要です。

Roquette とその処理者との間のデータ保護条項および / またはデータ保護契約を特定した契約により、当社の義務、責任、その両方を確実に理解することができます。また、契約は GDPR の遵守に役立ち、説明責任の原則で求められる当社の遵守を個人や規制当局に示すのに役立ちます。

処理業者を使用する場合、管理者としてどのような責任と義務がありますか?

私たちは、その処理が GDPR の要件を満たし、データ主体の権利を確実に保護するために、適切な技術的および組織的措置を実施することを十分に保証できる処理業者のみを使用しなければなりません。

管理者として、当社は、GDPR およびその他の施行中のデータプライバシー法の全体的な遵守、およびその遵守の実証に第一義的な責任を負います。これが達成されない場合、当社は法的手続きにおいて損害賠償責任を負うか、罰金その他の罰則または是正措置の対象となる可能性があります。

GDPR では何が新しくなりましたか?

GDPR は、現行のデータ保護法におけるデータ保護原則（適切なセキュリティ対策）の遵守を証明する手段にとどまらず、管理者と処理者間の書面による契約を要件としています。

これらの契約には、具体的な最低期間を含める必要があります。これらの条項は、処理業者が実施する処理が、個人データの安全保持に関連する要件だけでなく、GDPR のすべての要件を満たすように設計されています。

ルール	OneDoc 基準	GDPR 基準
• 下請業者との情報セキュリティおよびデータ保護条項の統合。	DIDPGR007EN 規則 4	第 32 条
• 請負業者のセキュリティ	DSUG016EN	

契約に含める必要があるものは何ですか?

契約書には以下が記載されている必要があります:

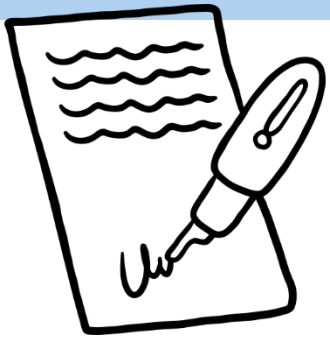
- ☑ 処理の対象と処理期間、
- ☑ 処理の性質および目的、および
- ☑ 個人データの種類とデータ主体のカテゴリー、および
- ☑ 管理者の義務と権利についての説明。

契約には、以下に関する具体的な条件または条項も含まれていなければなりません。

- ☑ 管理者の文書化された指示に基づく処理
- ☑ 機密保持の義務、および
- ☑ 適切なセキュリティ対策
- ☑ 下請けの処理業者を使用
- ☑ データ主体の権利、
- ☑ 管理者を支援することと、
- ☑ 契約終了に関する条項、および
- ☑ 監査および検査

私たちは従業員をトレーニングし、社内プロセスを改善します。

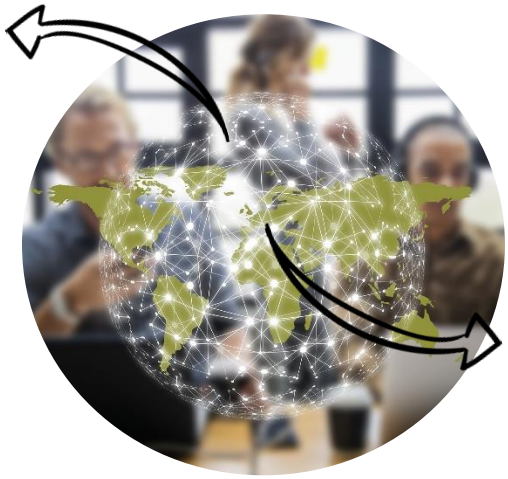
- GDPR 対応下請けデータ保護ガイド
- データ処理契約のテンプレートは、当社のプライバシー管理システムでご利用いただけます：OneTrust@Roquette> ベンダーリスク管理モジュール。



データ転送に関する同意

データ転送とは、個人データ保護法が適用されない他国での処理を目的とした、個人データの通信、コピー、転送（サーバーのホスティング、電子メールによる添付ファイルの送信、リモートアクセスツール、画面共有など）を指します。

私たちはこれまで以上に相互につながっています。グローバルに事業を展開する Roquette にとって、データの国際的なやり取りは日常業務に欠かせない要素です。例えば、Roquette 社は、従業員の個人データを海外でホスティングされたクラウドサービスに保管し、世界中に設立された子会社間で従業員や顧客の個人データを共有しています。



GDPR やその他の現行のデータ保護法は、このような国際的なデータ移転にどのような影響を与えるのでしょうか?

私たちの責任:

処理中であるか、または第三国もしくは国際機関への移転後に処理される予定の個人情報の移転は、以下の場合にのみ行われるものとします:

- 現地の法律が許可している場合、および/または、監督当局が、当該第三国、当該第三国内の地域もしくは 1 つ以上の特定分野、または当該国際機関が適切なレベルの保護を保証していると決定した場合、またはその許可を与えた場合、および/または
- 法的措置が講じられる場合（例：欧州議会および理事会指令 95/46/EC 等に基づき、第三国に設立された処理業者への個人データの移転に関する拘束力のある企業規則または標準契約条項）

ルール	OneDoc 基準	GDPR 基準
• 個人データを第三国または国際機関に転送するための措置を講じる	DIDPGR002EN 規則 5	第 44 条から第 50 条まで

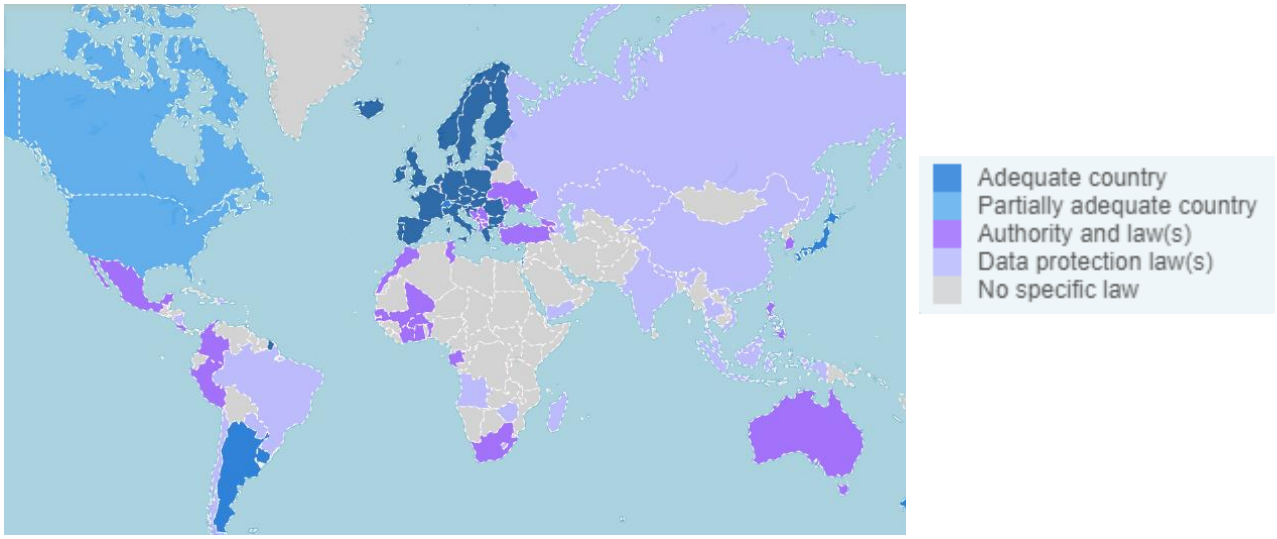
いずれの場合も、まず DPO に連絡してください。

個人データを転送できる国とその条件は？

概要については、次のマップを参照してください。

https://www.cnil.fr/en/data-protection-around-the-world.

このマップでは、各国のデータ保護レベルを確認できます。



私たちは従業員をトレーニングし、社内プロセスを改善します。

- 当社のデータ処理契約書テンプレートを含むデータ転送契約セクション。
- この FAQs は、第三国に設立された処理業者への個人データの移転に関する標準契約条項に関する EU 委員会決定の発効によって提起されたいくつかの問題に対処するためのものです。

3 ネットワーク および監督当局との関係における当社の基準

データ保護オフィサー

グループはデータ保護オフィサーを任命しています。

データ保護オフィサー（DPO）は、社内のコンプライアンスを監視し、当社のデータ保護義務について通知および助言し、データ保護影響評価（DPIA）に関する助言を提供、データ主体および監督当局の窓口として活動します。

DPOは、独立したデータ保護の専門家であり、十分なリソースを備え、最高経営レベルに報告する必要があります。

DPOはコンプライアンスを証明するのに役立ち、アカウンタビリティ（説明責任）強化の一環です。

DPO のタスク	OneDoc 基準	GDPR 基準
• DPOは、GDPRおよびその他のデータ保護法の遵守、当社のデータ保護ポリシー、啓発、トレーニング、および監査を監視することを任務としています。	MADPGROO1EN 個人情報保護マニュアル	GDPR 第 39 条 データ保護責任者の職務
• 当社は、当社のデータ保護義務に関するDPOの助言およびDPOが提供する情報を考慮します。		
• DPIAを実施する際には、プロセスを監視するDPOの助言を得ます。		
• DPO は監督当局の連絡窓口としての役割を果たします。		
• DPO は、業務を遂行する際、処理業務に関連するリスクを適切に考慮し、処理の性質、範囲、状況、目的を考慮します。		

グループDPOは、GDPRの適用日である2018年5月25日にCEOからCNILに指定されました。

DPO のアクセス可能性:

- 当社のデータ保護オフィサーである Jennifer Godin は、当社の従業員、個人、および監督当局の窓口として簡単にアクセスできます。
- 当社は DPO の連絡先情報を公表し、監督当局に通知しました。

  ☑ https://www.Roquette.com/data-protection

Your point of contact

Our Group Data Protection Officer is a single point of contact for our employees, individuals and the Supervisory Authorities concerning all privacy and data protection topics.

Jennifer Godin, Group Data Protection Officer
Roquette Frères, Legal & Compliance
Rue de la Haute Loge, 62136 Lestrem France

Email to DPO@roquette.com

以下の場合は DPO に連絡してください。

- ☑ 個人情報の取り扱いについて
- ☑ データ主体の要求
- ☑ 個人情報の違反
- ☑ アドバイスやサポートが必要な場合

私たちは従業員を教育し、社内プロセスを改善します。

データ保護ネットワーク

各部門への連絡役および現地 DPO またはコーディネーターは、それぞれグループデータ保護オフィサーが各事業部門およびサポート部門において個人データ保護規則を実施し、当グループが事業を展開する各国の関連法規のデータ保護要件を遵守するためのネットワークです。

現地 DPO/コーディネーターは、少なくとも以下の業務を行います：

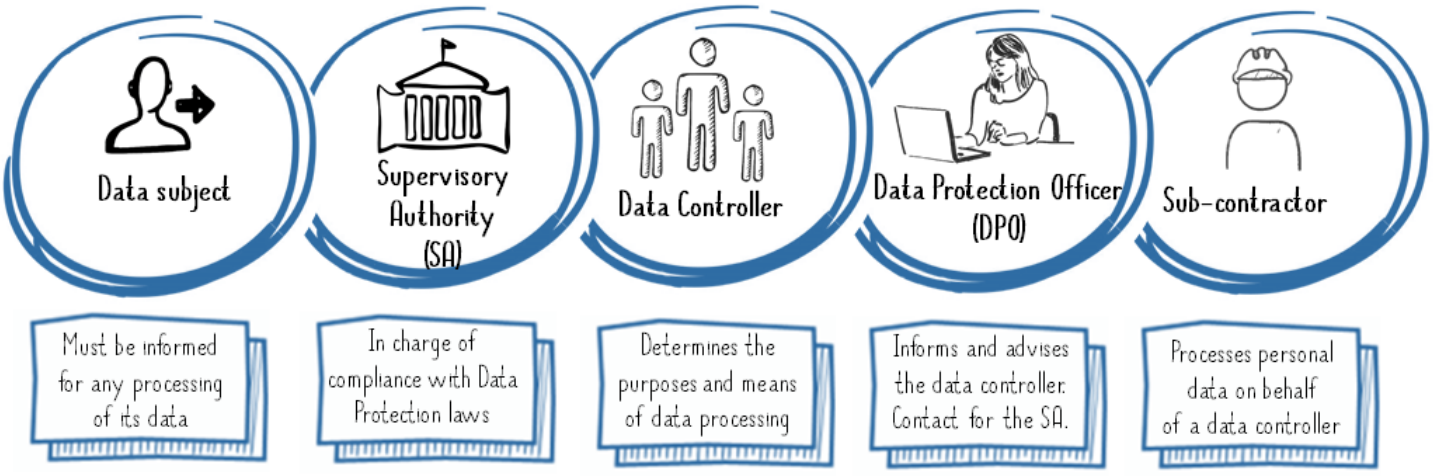
- Roquette'sグループのDPOが定めるRoquetteの個人情報保護ポリシーに従った義務、およびデータ保護に関する各地域の適用法の要件について、各地域に通知し、助言すること。
- 必要に応じてRoquetteグループのDPOの支援を受けながら、データ保護に関する地域の法律、その他の法律および適用される規制、ならびに個人データ保護に関するポリシーの遵守状況を監視すること。
- データ保護インパクト評価に関して要請があれば現地で助言を提供し、その実績を監視すること。
- 地域の監督当局と協力すること。
- 処理に関する問題に関してRoquetteのグループDPOの窓口となり、その他の問題に関して適切な場合にはRoquetteのグループDPOに相談すること。
- RoquetteのグループDPOに自身の活動を報告し、グループデータ保護管理システムに貢献すること。

私たちは従業員を教育し、社内プロセスを改善します。

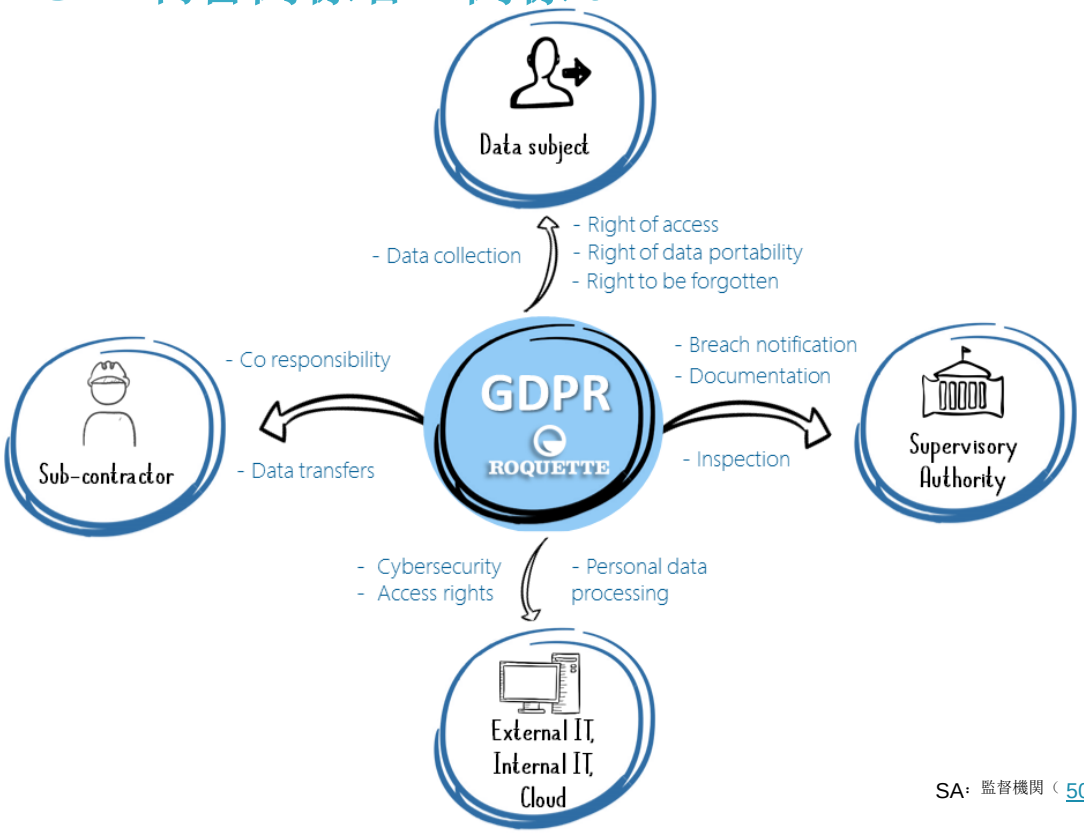
毎年開催される PDP セミナーは、データ保護とプライバシーに関する貢献者のネットワークが集まる場です。

& 利害関係者

新しいプレイヤーは誰ですか？



これらの利害関係者の関係は？



SA：監督機関（50 ページを参照）

監督当局

世界中の多くの国でデータ保護法が制定され、独立したデータ保護機関が設置されています。

データ保護機関（DPA）

これらの当局は、プライバシーと情報の自由に関する国の独立した規制当局です。データ対象者が組織の保有する情報にアクセスし、個人情報を保護される権利を促進し、支持します。

GDPR の文脈における監督機関の役割は何ですか?

各加盟国は、個人データ処理範囲におけるデータ主体の基本的権利と自由を保護し、EU 域内における個人データの自由な流れを促進するため、個人データおよびプライバシー法の適用を監視する責任を負う 1 つ以上の独立した公的機関を規定するものとします。

GDPR の文脈において、すべての EU 加盟国にはデータ保護当局があり、一般的にその加盟国内の利害関係者の主な窓口となっています。

GDPR が EU 全域で一貫した形で適用されるようにするため、各監督当局は他の監督当局や欧州委員会と協力しなければなりません。

各監督当局は、個人データ処理に関連するリスク、規則、保護措置、および権利に関する国民の認識と理解を促進しなければなりません。

また、データ保護法違反があった場合の相談先でもあり、組織の立場からのアドバイスや具体的な質問、支援も行っています。

監督当局（SA）の責務は以下の通りです：

- 罰金を含むルールの適用を徹底させること
- 必要であれば、ガイドラインなどでルールの適用を明確化
- 企業を含むすべての利害関係者との対話文化の促進
- 協力し合うこと

CNIL：フランス情報自由委員会/ Commission Nationale de l'Informatique et des Libertés - フランス DPA。

主管官庁

- 管理者または処理者の主な事業所の監督当局は、主管官庁として機能する必要があります他の関係当局と協力する必要があります。
- 主管監督官庁の特定は、管理者または処理者が個人データの国境を越えた処理を実施している場合にのみ関連します。

「主管監督官庁」を特定するには？

EU における主管理者の中枢管理場所の特定。
中央管理地が所在する国の監督当局は、管理者の主管官庁です。

CNIL は *Roquette の主任監督官庁*です。

GDPR 制裁メカニズムは実際にどのように機能しますか？

管理

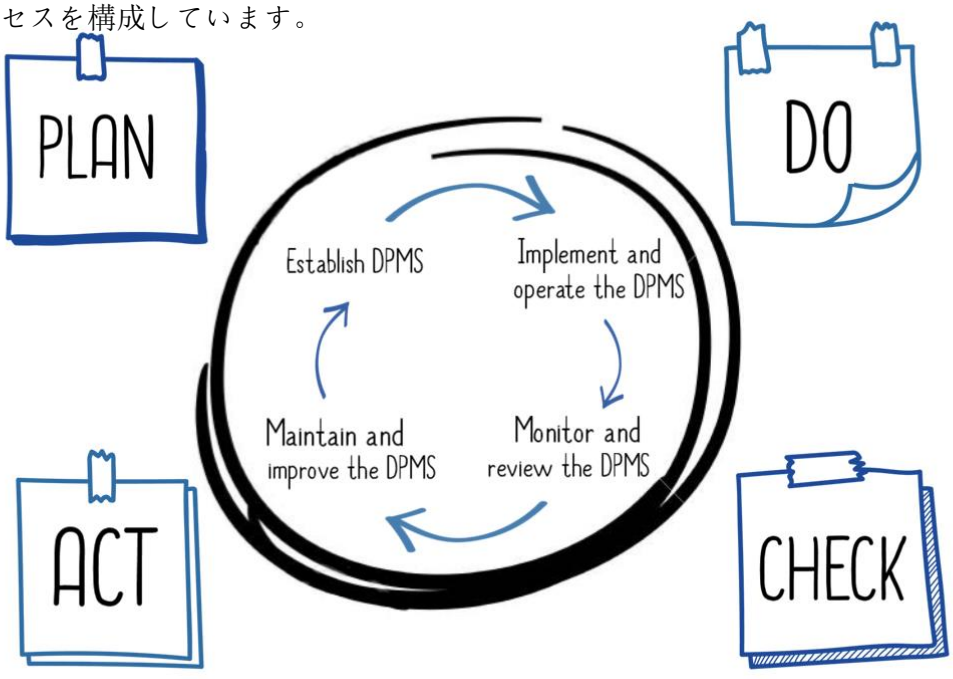
「**データ保護組織**は主に、データ保護責任者、各拠点および各機能ごとのコーディネーター、データ管理者としての最高経営責任者、個人データ処理の実施責任者としてのグローバル機能責任者、および処理者としての下請業者を中心に構成されています。」 [MDPG001EN]

当社は、Roquetteの個人情報保護マネジメントシステム**DPMS**（データプロテクション・マネジメント・システム）の確立、実施、運用、監視、見直し、維持、改善のためにプロセスアプローチを採用しています。

本ガバナンスで定義する個人情報保護管理のプロセスとアプローチは、その利用者に以下の重要性を促すものです：

1) Roquetteのデータ保護要件、およびデータ保護に関する指令と手順を確立する必要性を理解すること。
2) Roquetteの全体的な事業リスクとの関連において、Roquetteのデータ保護リスクを管理するための統制を実施し、運用すること。
3) DPMSのパフォーマンスと有効性のモニタリングとレビュー、および
4) 客観的な測定に基づく継続的な改善。

私たちは「Plan-Do-Check-Act」（PDCA）モデルを採用し、すべてのデータ保護管理システム（DPMS）プロセスを構成しています。



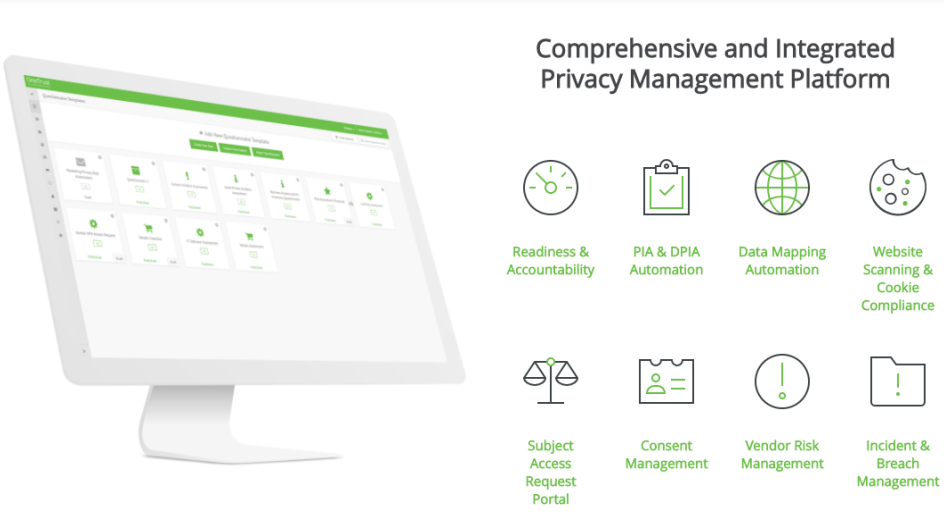
私たちのアプローチ：

GDPR コンプライアンスプログラムの焦点：

- コンプライアンスを確保するために、組織がどのようにデータを収集、保存、利用、転送しているかを理解
- 組織内のコンプライアンス文化の創造
- プライバシー影響評価の実施
- データ侵害への備え
- 個人情報保護プログラムへのリソースの割り当て
- データ保護管理システムの導入（Plan - Do - Check - Act）

これらの目標を達成するために、私たちはプログラムの一環として、次のことを掲げています：

- データ保護ポリシーと関連するガバナンスとドキュメンテーションを定義
- 処理の見直し、データ漏えいの管理、契約書の見直し、データ保護に関する条項、データ移転契約などの GDPR 対応プロジェクトを管理
- GDPR に対応した個人情報管理ソフトウェアを導入



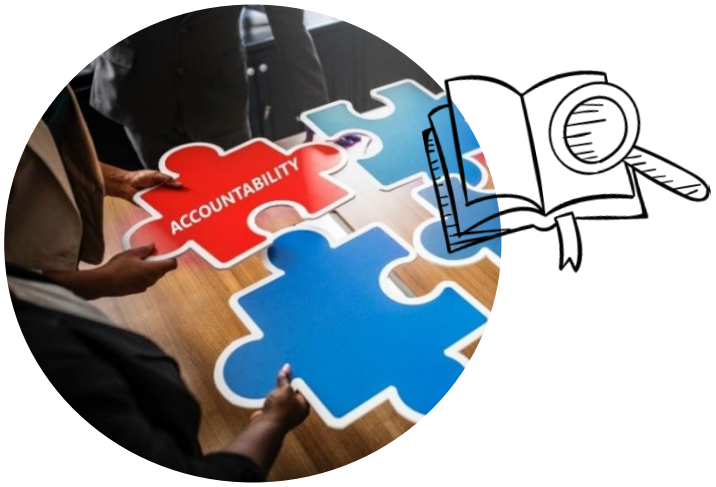
この管理プラットフォームの主な特徴は以下の通りです：

- データ処理レジスタ（データマッピング）のメンテナンス
- 処理に伴うリスク管理（PIA 等より）
- 請求および権利（アクセス、修正、異議申し立てなど）の管理
- インシデントおよびデータ漏洩の管理
- **コンプライアンス文書の管理**

説明責任

説明責任は　　、データ保護の原則の一つです。GDPR　　を遵守する責任を負い、コンプライアンスを実証する必要があります。

説明責任が重要なのはなぜですか?



個人データの取り扱いに責任を持ち、人々の権利を保護するために講じた措置を示すことは、法令遵守の向上につながるだけでなく、当社の競争力にもつながります。説明責任は、私たちがいかに人々のプライバシーを尊重しているかを示し、それを証明する絶好の機会です。これにより、人々の信頼を育み、維持することができるのです。

さらに、何か問題が発生した場合、私たちが積極的にリスクを考慮し、対策と安全策を講じたことを示すことができれば、潜在的な強制措置に対して緩和策を講じることができます。その一方で、もし私たちが優れたデータ保護慣行を示すことができなければ、罰金や風評被害を受ける可能性があります。

説明責任の原則を遵守することは具体的に何を意味しますか?

個人データの処理には注意義務があり、その保護のために具体的で実践的な措置を講じる必要があります。説明責任の原則を遵守することは、以下を意味します。

- プライバシーに関連するすべての指令、手順、慣行（「ポリシー」）を文書化し、適切に伝達すること。
- 組織内の特定の個人（その個人は、必要に応じて組織内の他の個人に委任することができます）に、ポリシーを実施するタスクを割り当てること。
- 個人データを第三者に移転する場合、第三者の受領者が、契約上、または強制的な内部方針などのその他の手段を通じて、同等レベルのプライバシーおよびデータ保護を提供する義務を負うことを確認します（適用される法律には、国際的なデータ移転に関する追加要件が含まれる場合があります）。

- 個人データにアクセスできるデータ管理者の従業員に対する適切なトレーニングの実施。
- データ対象者が利用できる効率的な内部クレーム処理および是正手続きの設定。
- データ対象者に重大な損害を与える可能性のあるプライバシー侵害について（法執行機関と協力している場合など、禁止されている場合を除く）、解決のために取られた措置と同様にデータ対象者に通知すること。
- 一部の管轄区域（データ保護当局など）で要求され、かつリスクのレベルに応じて、プライバシー侵害についてすべての関連プライバシー利害関係者に通知すること。
- プライバシー侵害が発生した場合、権利を侵害されたデータ対象者が適切かつ効果的な制裁措置および/または是正措置（修正、抹消、返還など）を利用できるようにすること。
- 自然人のプライバシー状態を何事もなかったかのように戻すことが困難または不可能な場合の補償手続きの検討。

チェックリスト：

☑ 私たちは、GDPR を遵守する責任を、最高経営責任者レベルおよび組織全体で負います。
☑ 当社は、GDPR を遵守するための措置を証拠として保管します。

当社は、以下のような適切な技術的および組織的措置を講じています：

☑ データ保護規則の採用と実施
☑ 「設計とデフォルトによるデータ保護」アプローチを採用し、処理業務のライフサイクル全体にわたって適切なデータ保護措置を講じる。
☑ 当社に代わって個人データを処理する組織と書面による契約を締結すること
☑ 当社の処理活動に関する文書の管理
☑ 適切なセキュリティ対策の実施
☑ 個人データの侵害を記録し、必要に応じて報告すること。
☑ 個人の利益に対して高いリスクをもたらす可能性がある個人データの使用について、データ保護影響評価を実施すること。
☑ データ保護オフィサーの任命、および
☑ 関連する行動規範を遵守し、認証スキームに登録する（可能な場合）。

☑ 当社は、適切な間隔で説明責任対策をレビューし、更新します。

文書化

文書化とは何ですか?

当社は、処理目的、データの共有および保持などの領域を含む、当社の処理活動の記録を保持することが義務付けられており、これを**文書化**と呼んでいます。

当社の処理活動を文書化することは、それ自体が法的要件であるためだけでなく、優れたデータ管理を支援し、GDPR の他の側面および施行中のデータ保護法への準拠を証明するのに役立つため、重要です。

処理活動の文書化 - 要件

- ☑ 当社は、当社が処理する個人データの管理者として、GDPR 第 30 条 1 項に基づき該当するすべての情報を文書化します。
- ☑ 当社は、処理活動を書面で文書化します。
- ☑ 当社は、さまざまな情報間の有意義なリンクにより、詳細な方法で処理活動を文書化します。
- ☑ 当社は、当社が処理する個人データの定期的なレビューを実施し、それに応じて文書を更新します。

処理活動の文書化 - 行動規範

- ☑ 当社は、情報を簡単に追加、削除、修正できるように、処理活動を電子形式で文書化します。

処理活動を文書化する準備をする際、当社は以下を行います。

- ☑ 組織が保有する個人データを確認するために情報監査を実施する。
- ☑ 当社のデジタル、セキュリティ、プライバシーツールを通じてアンケートを利用し、組織全体のスタッフと話し合い、処理活動のより完全な概要を得る。
- ☑ データ保持、セキュリティ、共有などの分野に対処するため、当社のポリシー、指令、手順、契約、および合意を見直します。

当社の処理活動の記録の一部として、当社は以下の事項を文書化し、または文書にリンクします:

- ☑ プライバシー通知に必要な情報
- ☑ 必要な場合、同意の記録
- ☑ 管理者 - 処理者間の契約
- ☑ 個人データの場所
- ☑ データ保護影響評価レポート
- ☑ 個人データ侵害の記録
- ☑ データ主体の請求の記録

チェックリスト:

データ保護に関する文書はどこにありますか?

ONE
Global Function
Data Protection

Privacy & Data Protection

"Data Protection is relevant to and the responsibility of everyone in our organization"

Content

- Laws and regulations
- Information and awareness
- Best practises and policies

ONE
Community
Data Protection Network

Data Protection Network

"We are all actors in the protection of personal data"

Content

- Personal Data Protection Policy
- Data Protection Management System
- Local Legislation
- Human resources
- Global Digital
- Legal & Compliance
- Internal Audit & Control
- GBU & Commercial
- Innovation, R&D
- Global Security
- Insurance & Risk Management

OneTrust
Privacy Management Software

OneTrust
Privacy Management Software
@ ROQUETTE

"Our Privacy Management tool dedicated to Privacy Security & Third Party Risk"

CULTURE → COMPLIANCE → ACCOUNTABILITY

プライバシー影響評価

プライバシー影響評価（PIA）とは、個人データの処理について説明し、その必要性と比例性を評価し、個人データの処理に起因する自然人の権利と自由に対するリスクを評価し、それらに対処するための措置を決定することによって、リスク管理を支援するために設計されたプロセスです。

略語「PIA」は、**プライバシー影響評価（Privacy Impact Assessment**）および**データ保護影響評価（Data Protection Impact Assessment**：DPIA）と同じ意味で使用されます。

PIA はどのように実施されますか?

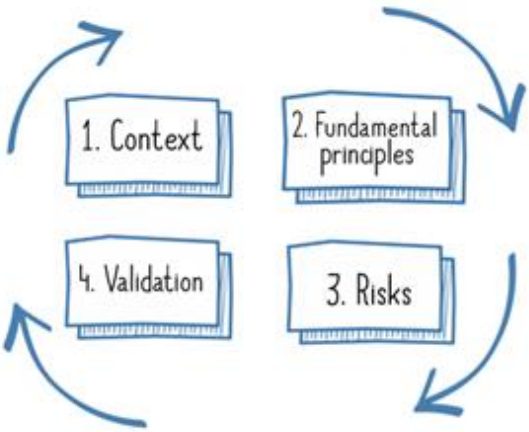
PIA を実施することで実施されるコンプライアンスアプローチは、2 つの柱に基づいています。

1) **基本的権利と原則** は「交渉不可」であり、法律で定められており、リスクの性質、重大性、可能性にかかわらず尊重されなければなりません。
2) **データ主体のプライバシーリスクの管理 。**個人データを保護するための適切な技術的および組織的管理を決定します。

Compliance approach using a PIA

まとめとして、 PIA を実行するには、以下を行う必要があります。

1) 検討中の個人データの処理 状況 を定義し、説明すること。
2) 基本原則 の遵守を保証する管理を分析する。処理の比例性と必要性、およびデータ主体の権利の保護。



General approach for carrying out a PIA

3) データセキュリティに関連するプライバシー リスクを評価し、それらが適切に処理されていることを確認する。
4) 手元にある以前の事実を考慮して PIA の 検証を正式に文書化するか、以前のステップを改訂する。

これは継続的な改善プロセスです。したがって、許容可能なプライバシー保護システムを達成するには、いくつかの繰り返しが必要になる場合があります。また、経時的な変化（状況、管理、リスクなど）の監視も必要です。たとえば毎年、大幅な変更が発生するたびに更新します。

このアプローチは、個人データの新たな処理が設計され次第、直ちに実施されるべきです。このアプローチを最初に導入することで、必要かつ十分なコントロールを決定し、コストを最適化することが可能になります。逆に、システムを構築し、統制した後に実施すると、その選択に疑問が生じる可能性があります。

私たちの責任:

- 特に新技術を使用した処理において、処理の性質、範囲、背景および目的を考慮した結果、個人の権利および自由に対して高いリスクが生じる可能性がある場合、管理者である Roquette は、処理に先立ち、想定される処理業務が個人情報の保護に与える影響の評価を実施するものとします。
- プロジェクトオーナーは、データ保護影響評価を実施する際に、指定されたデータ保護オフィサーの助言を求めるものとします。

ルール	OneDoc 基準	GDPR 基準
• 高リスクの場合に PIA を実施する	DIDPGR003EN 規則 1	第 35 条
• PIA の内容	DIDPGR003EN 規則 2	
• PIA に関する DPO のタスク	DIDPGR003EN 規則 3	
• PIA のレビュー	DIDPGR003EN 規則 4	

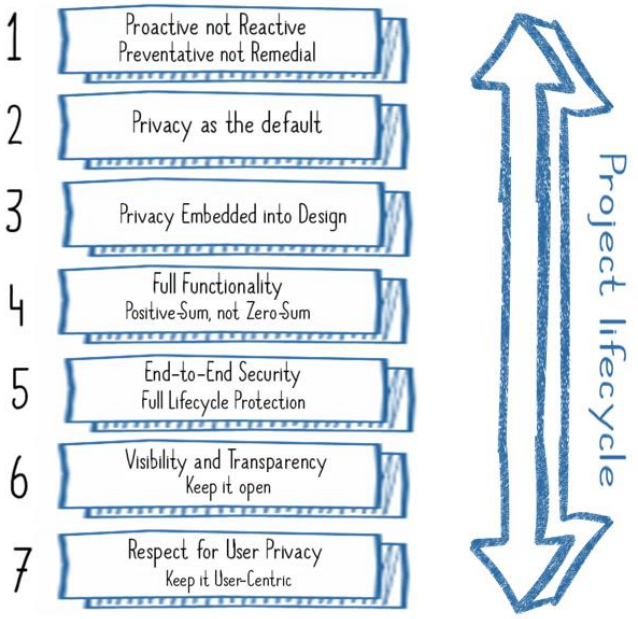
私たちは従業員をトレーニングし、社内プロセスを改善します。

- プロジェクトと契約における、セキュリティとプライバシーの見直しに関する学習。
- プライバシー影響評価テンプレートは、必要に応じてプライバシー管理ソフトウェア OneTrust@Roquette で自動的に起動します。

詳細： CNIL PIA Methodology、2018 年版 - https://www.CNIL.fr/en/home

デザイン&デフォルトによるプライバシー

プライバシー・バイ・デザインとは、与えられたシステム、ビジネスプロセス、または設計仕様の設計、運用、管理にプライバシーを組み込むことを意味します。



デザインによるデータ保護とは？

データ保護法には、データ主体のプライバシーを保護するための基本原則が含まれています。

設計上およびデフォルトで行われるデータ保護は、当社が使用する情報システムがこれらのデータ保護原則を満たし、データ主体の権利を保護することを保証するのに役立ちます。

私たちの考え：

Roquette は、さまざまな運用および管理タスクを実行するために情報システムとデータベースに依存しています。これらの情報システムの大部分は個人データを処理するため、規制を完全に遵守することが非常に重要です。

データ保護の問題を真剣に受け止めている企業は、信頼を獲得します。

したがって、強力なデータ保護対策は競争上の優位性をもたらすものです。

経営陣のコミットメントは、調達とソフトウェア開発において、設計によるデータ保護の原則を適用する上で不可欠です。

経営陣は、このタスクに十分なリソースを確保する必要があります。

開発プロセス全体にわたってデータ保護を考慮することは、既存のソフトウェアを変更するよりも費用対効果が高く、効率的です。

私たちの責任:

GDPR に基づき、設計によるデータ保護は初めて法的義務となりました。つまり、情報通信システムと技術の設計仕様とアーキテクチャに、データ保護とプライバシーを組み込む必要があります。

Roquette はデータ管理者として、ソフトウェア開発中、およびシステム、ソリューション、サービスを発注する際に、設計によるデータ保護に関する要件を遵守する必要があります。

したがって、サプライヤーとの契約を締結するとき、およびコンサルタントを利用するときも、要件を考慮する必要があります（ 下請け業者に対する当社の基準）。

ルール	OneDoc 基準	GDPR 基準
• 設計とデフォルトによるセキュリティ、プライバシー、データ保護	DIDPGR007EN ルール 3	第 25 条

チェックリスト:

- ☑ データ保護影響評価（DPIA）のレビュー
- ☑ 機密性の高い個人データの収集と処理の必要性を回避、制限、または最小化する
- ☑ ユーザーインターフェース内の不要な機能や個人データの露出を制限し、最小限に抑える
- ☑ 可能な限り、個人データを匿名化または偽名化する
- ☑ すべてのプライバシー保護設定はデフォルトでオンにする必要があります
- ☑ あるウェブサイトから別のウェブサイトへの追跡は、デフォルトで無効にする必要があります
- ☑ ソフトウェア内のメニューから、同意を撤回できるようにします。同意が撤回された場合、個人データの収集は停止しなければなりません。
- ☑ 設定は、データ対象者が、プライバシーにあまり配慮していない設定に積極的に「変更」することを、意識的に選択しなければならないようなメニューで提示すべきです。
- ☑ デバイス追跡はデフォルトで無効にする必要があります

私たちは従業員を教育し、社内プロセスを改善します。

- 当社のコミュニティ「データ保護ネットワーク」に関するガイドライン。
- 手順: プロジェクトと契約における、セキュリティとコンプライアンスのレビュー。
- HR プラットフォームでの学習。

データ漏えいに関する通知

個人情報漏えいとは何ですか?

個人情報の漏えいとは、送信、保存、またはその他の方法で処理された個人情報の、偶発的または違法な破壊、紛失、改ざん、不正な開示、または個人情報へのアクセスにつながるセキュリティ違反を意味します。

つまり、侵害は個人データ の 損失だけではありません。

例:

- クライアントデータベースの喪失
- 従業員の業績評価の開示

私たちの責任:

私たちは、個人情報の漏洩がデータ対象者に与える影響を最小限に抑え、再発を防止するための規定を適用しなければなりません。

ルール	OneDoc 基準	GDPR 基準
• 個人情報保護責任者への個人情報漏えいの通知。	DIDPGR008EN 規則 1	第 33 条
• 個人情報漏えいの監督当局への通知。	DIDPGR008EN 規則 2	
• 個人データの侵害をデータ主体に通知。	DIDPGR008EN 規則 3	第 34 条

情報漏えいの報告期限は?

当社は、通知可能な違反について、監督当局に過度の遅滞なく報告する必要があり、遅くとも違反に気づいてから 72 時間以内に報告する義務があります。

監督当局にどのような違反について通知する必要がありますか?

違反が個人の権利と自由に対するリスクにつながる可能性が高い場合にのみ、関連する監督当局に通知する必要があります。違反に対処しなければ、個人に重大な悪影響を及ぼす可能性があります。例:

- その結果、差別が生じる内容
- 評判へのダメージ
- 財務上の損失
- 機密性の喪失またはその他の重大な経済的または社会的不利益

私たちはケースバイケースでこれを評価しなければならず、監督当局に違反を報告するという決定を正当化できる必要があります。

個人への通知は、いつまでに行う必要がありますか?

違反行為が個人の権利と自由に対して**高いリスク**をもたらす可能性がある場合、当社は過度の遅滞なく関係者に直接通知しなければなりません。

以下の場合、違反について個人に通知する義務はありません。

- 当社は、侵害の影響を受けた個人データに適用される適切な技術的および組織的対策を実施した場合。
- 個人の権利と自由に対する高リスクがもはや起こり得ないことを保証する措置を講じた場合。
- 不釣り合いに多大な労力を要する場合。

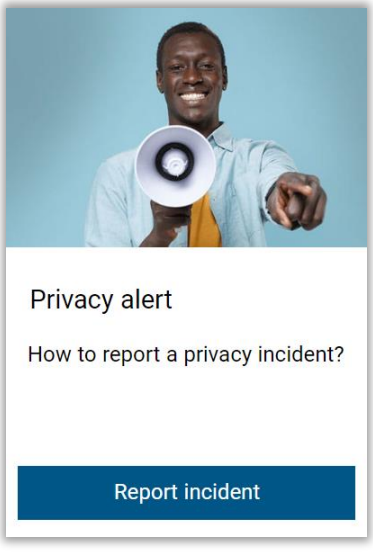
違反の通知が、不相応な労力を伴う場合、私たちは、一般への通知など、他の同等の効果的な方法で、個人に対して情報を提供しなければなりません。

データ漏えいが発生した場合は、誰に連絡すればよいですか?

dpo@Roquette.com のデータ**保護オフィサー**に連絡するか、「 プライバシー警告 」ウェブフォームを使用してインシデントを報告してください。

コンプライアンス違反の可能性を報告する必要がある場合は、通常の連絡先に連絡するか、機密の Roquette アラートシステムを通じて問題を報告することができます: Speakup©

SpeakUp



モニタリング&レビュー

私たちの考え:

Roquette は以下に取り組んでいます:

- ☑ データ保護要件に関する法的および技術的な**監視**の保証
- ☑ データ保護管理システム（DPMS）の**見直し**と**改善**

これは、規制や技術の進化、およびサービスの内部制約を考慮するためです。
[DIDPGR009EN]

私たちの責任:

ルール	OneDoc 基準	GDPR 基準
• 個人データの保護に関する法的および技術的な監視とレビューを保証	DIDPGR009EN 規則 1	行動規範
• DPMS およびデータ保護指令の実施を定期的に監視	DIDPGR009EN 規則 2	
• 個人情報保護ポリシーおよび DPMS の文書を定期的にレビュー	DIDPGR009EN 規則 3	

私たちは従業員を教育し、社内プロセスを改善します。

プライバシープログラムの設計とサポート

規制に関する調査ソフトウェア：

当社は、規制の動向を監視してリスクを軽減し、グローバルコンプライアンスを達成するために設計された一連の個人情報保護ソリューションを提供するプラットフォームを使用しています。

- ☑ 規制の動向調査
- ☑ 国境を越えた比較チャート
- ☑ ガイダンスノート
- ☑ GDPR ポータル
- ☑ テンプレートとチェックリスト
- ☑ 分析サービスのお問い合わせ
- ☑ 法的調査

データ保護管理システムの監査とレビュー：

DPMS のインプットが正しいかどうかを内部監査します：

- ☑ 本ガイド、方針、および適用される法律または規制の要件に準拠していること。
- ☑ 効果的に実施され、維持されていること。
- ☑ 期待どおりに実行されていること。

当社は DPMS のマネジメントレビューを実施し、適用範囲が適切であり、 DPMS プロセスの改善が特定されていることを確認します。

これを行うには、以下の事項を利用します：

- ☑ DPMS の目的、管理、プロセス、手順
- ☑ 以前のコンプライアンス監査および管理の結果
- ☑ 利害関係者からのフィードバック
- ☑ 組織内で DPMS のパフォーマンスと有効性を改善するために使用できる技術、製品、または手順。
- ☑ 予防措置と是正措置のステータス
- ☑ 以前のリスク評価で十分に対処されていない脆弱性または脅威。
- ☑ 有効性測定からの結果、

- ☑ 前回のマネジメントレビューからのフォローアップ活動
- ☑ DPMS に影響を及ぼす可能性のある変更
- ☑ 改善のための推奨事項。

基準文書

- [行動規範] Roquette グループ行動規範
- [GDPG001EN] データ保護に関する定義の用語集
- [MDPG001EN] 個人情報保護マニュアル
- [DIDPGR001EN] プライバシーとデータ保護の尊重文化に関する指示
- [DIDPGR002EN] 個人データ処理の合法性に関する指示
- [DIDPGR003EN] プライバシー影響評価に関する指示
- [DIDPGR004EN] 機密データの処理に関する指示
- [DIDPGR005EN] 処理活動の記録に関する指示
- [DIDPGR006EN] 人権の遵守に関する指示
- [DIDPGR007EN] 個人データのセキュリティに関する指示
- [DIDPGR008EN] 個人データ侵害の通知に関する指示
- [DIDPGR009EN] 個人情報保護管理システムのレビューに関する指示
- [DIDPGR010EN] 警告管理システムのプライバシーとデータ保護に関する指示
- [DISUGR001EN] 情報保護と機密保持に関する指示

参考文献

[EU 憲章]欧州連合基本権憲章 2010/C 83/02.

[GDPR]個人データの処理に関する自然人の保護および当該データの自由な移動に関する 2016 年 4 月 27 日の欧州議会および理事会の規則（EU）2016/679、および指令 95/46/EC（一般データ保護規則）の廃止。

[DP-Act] 1978 年 1 月 6 日付フランス情報保護法第 78-17 号、改正。

[WP29 - ガイドライン]管理者または処理者の主管監督官庁を特定するためのガイドライン｜WP 244 改訂 01 版（2017 年 4 月 5 日）。

[WP29- ガイドライン] データ保護影響評価（DPIA）および規則 2016/679 の目的上、処理が「高リスクになる可能性が高い」かどうかの判断に関するガイドライン｜WP 248 改訂 01 版（2017 年 10 月 13 日）

[WP29- ガイドライン] 規則 2016/679｜WP 253（2017 年 10 月 21 日）の目的のための行政罰金の適用と設定に関するガイドライン。

[WP29- ガイドライン] 規則 2016/679 の目的のための、自動化された個人の意思決定とプロファイリングに関するガイドライン｜WP 251 改訂 01 版（2018 年 2 月 13 日）。

[WP29 - Guidelines] データ保護責任者（DPO）に関するガイドライン｜WP 243 改訂 01 版（2017 年 4 月 5 日）

[WP29- ガイドライン] 規則 2016/679 に基づく透明性に関するガイドライン｜WP260 改訂 01 版（2018 年 4 月 11 日）

[WP29- ガイドライン] 規則 2016/679 に基づく同意に関するガイドライン｜WP259 改訂 01 版（2018 年 4 月 11 日）

[EDPB - Opinion]刑事事件における電子証拠の欧州的作成・保全命令に関する欧州委員会提案に関する意見書 23/2018（第 70.1.b 条）（2018 年 9 月 26 日）

[EDPB - Opinion]日本における個人データの適切な保護に関する欧州委員会の実施決定案に関する意見書 28/2018（2018 年 12 月 5 日）

[EDPB - Opinion]DK SA から提出された標準契約条項案（GDPR 第 28 条 8 項）に関する意見書 14/2019（2019 年 7 月 12 日）。

[EDPB- Recommendation] データ保護影響評価（規則(EU)2018/1725 の第 39 条(4)）の要件の対象となる処理業務の欧州データ保護監督者のリスト案に関する勧告 01/2019（2019 年 7 月 10 日）。

[EDPB - EDPS の共同回答] 個人データ保護に関する欧州法的枠組みへの米国クラウド法の影響に関する LIBE 委員会への EPDB-EDPS 共同回答（附属書）（2019 年 7 月 10 日）

[EDPB 意見] データ保護影響評価（GDPR 第 35 条 5 項）の要求から免除される処理業務に関するフランスの管轄監督当局のリスト案に関する意見 13/2019（2019 年 7 月 10 日）

出典

- フランス情報自由委員会（フランスデータ保護局）
    - https://www.cnil.fr/en/home
    - 2022 年 5 月
    - ライセンス：CC-BY-ND 3.0 FR
- 情報委員会事務局
    - https://ico.org.uk/
    - 2022 年 5 月
    - オープンガバメントライセンスに基づくライセンス
- 欧州連合
    - https://eur-lex.europa.eu
    - 1998-2022
- https://www.iso.org/home.html
- https://www.dataguidance.com/
- https://www.onetrust.com/
- https://www.corporatefiction.fr/
- https://pixabay.com/fr/service/license/

このガイドは英語版が基準となります。
この文書の翻訳には一定の解釈が必要な場合があります。
初版：2019 年 9 月
第 2 版：2022 年 5 月
出版：ROQUETTE FRERES
作成者：Jennifer Godin、データ保護責任者
編集デザイン＆グラフィック：コンプライアンス・オフィス
写真：無料でご利用いただけます

PUBLIC

ROQUETTE

Offering the best of nature™