

Getinge グローバルポリシー

## データ・プライバシー グローバルポリシー

ドキュメントオーナー	アンナ・ロンバーク
バージョン	v3
取締役会にて採択される	2023 年 4 月 26 日

### 1. 概要

このグローバルデータプライバシーポリシー（以下「**グローバル ポリシー**」）の目的は、主なデータプライバシー要件を定め、個人データの処理に関わる日常業務において、ゲティンゲの経営陣、社員、コンサルタントにガイドラインを提供することです。

ゲティンゲは、適用されるデータ保護法および規制に従って個人データを処理することを約束します。当社は、個人情報の保護を常に最重要視し、日々の業務に取り組んでいます。

このグローバルポリシーは、ゲティンゲを代表して行動するすべての従業員、取締役、ビジネスパートナーに適用されます。

### 2. 定義

本グローバルポリシーにおいて、以下の用語は、以下の意味を有します：

<b>データコントローラー</b>	単独で、または他の事業体と共同で、個人データの処理の目的および手段を決定する事業体を指します。
<b>データプロセッサ</b>	データ管理者に代わって個人データを処理する法人をいいます。
<b>データ保護影響評価 (Data Protection Impact Assessment)</b>	データ保護への影響という観点から、プロジェクト、プロセス、またはソリューションを評価するための体系的なプロセスです。
<b>データ保護法</b>	GDPR を含むがこれに限定されない、適用されるあらゆるデータ保護法および規制。
<b>データ対象</b>	個人データに関連する個人本人。
<b>GDPR</b>	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 であり、指令 95/46/EC を廃止している。

## 個人情報

データ・サブジェクトに関連するあらゆる情報。データ対象者とは、氏名、識別番号、位置情報、オンライン識別子、または自然人の身体的、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要素を用いて、直接的または間接的に識別することができる人をいいます。また、個人データには、勤務先の電子メールアドレスや担当者などの従業員の連絡先も含まれます。

## 個人情報漏えい

送信、保存、またはその他の方法で処理された個人データの偶発的または違法な破壊、損失、改ざん、不正な開示、またはアクセスにつながるセキュリティ違反。

## 個人情報の取り扱いについて

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操作または一連の操作（収集、記録、整理、構造化、保存、適応または変更、検索、相談、送信による使用開示、普及またはその他の利用可能化、調整または組み合わせ、制限、消去または破壊など）。また、処理には個人データの閲覧も含まれます。

## パーソナルデータの特別なカテゴリー

生存する自然人の人種または民族的出身、政治的意見、哲学的または宗教的信条、性的指向、労働組合への加入および活動、遺伝子または生体情報、ならびに健康または性生活に関するデータを直接的または間接的に示すすべての個人データです。

## 監督官庁

データ保護法の遵守を監視する責任を負う独立した公的機関です。

## 3. 範囲と目的

このグローバルポリシーは、すべてのゲティンゲ社、その子会社および共同事業（共同で「ゲティンゲ」）に対して有効であり、当社のすべての従業員、ならびにゲティンゲ社の敷地内またはゲティンゲ社の指示の下で働くコンサルタントおよび代理店職員（このグローバルポリシーではすべて「社員」と呼ぶ）に対して適用します。一般的なルールとして、このグローバルポリシーは、Getinge 社内のすべての個人データの処理に適用されます。本グローバルポリシーに定める場合に限りに、例外を適用します。

本グローバルポリシーは、以下を目的としています：

- 個人データおよび適用されるデータ保護法に関する一般的な知識
- ゲティンゲにとって最も重要な法的要件に関するガイダンス
- 個人データを処理する際のゲティンゲの要件
- ゲティンゲが個人データを処理する際に従うべき指示

当社は、このグローバルポリシーに基づき、個人情報保護法に従って個人情報を保護することを約束します。

## 4. 応用分野

### 適用範囲について具体的に

本グローバルポリシーは、以下に適用されます：

- a) 業務プロセスにおける個人データの処理
- b) 個人データを処理するために使用される IT 機能、ソリューションまたはサービス
- c) Outlook、PowerPoint、Word、Excel などのツール。
- d) ゲティンゲが第三者に代わって個人データの処理を含む製品またはサービスを提供する場合（例：病院に提供される IT ソリューション）。
- e) 本グローバルポリシーに記載されているように、Getinge がデータ管理者、データ処理者、および共同管理者のいずれかに該当するその他のすべての状況。

IT セキュリティに関する要件など、本グローバルポリシーに記載されている以外の要件が、特定の業務において必要となる場合があります。このグローバルポリシーに加えて、特定のゲティンゲチームに適用される個人データの処理に関する追加の指示およびガイドラインが存在する場合があります。

### 適用される法律、地域要件および逸脱事項

このグローバルポリシーは、欧州のデータ保護法および規制に基づいていますが、EU/EEA の外でも、すべてのゲティンゲの個人データ処理に関連し適用されます。このような処理に欧州のデータ保護法および規制が適用される理由は、例えば、次のようなものです：

- a) 処理は、EU/EEA 内に拠点を置くゲティンゲ本社が採用した手順、システム、ルーチン、または決定に関するものであること
- b) 処理が、EU/EEA 内のデータ対象者に提供される商品・サービス、またはデータ対象者の行動の監視に関連するものであること。
- c) EU/EEA の外にある企業は、EU/EEA に従業員がいるなどの理由で、EU/EEA に設立されているとみなされる。

現地のデータ保護に関する法律や規制が、このグローバルポリシーとは異なる、またはより厳しい要件を課す場合、Getinge は当該法律や規制を遵守するものとします。法律や規制がこのグローバルポリシーと矛盾する場合、より厳しい要求が優先されるものとします。詳しいガイダンスについては、データ・プライバシー・チームまでお問い合わせください。

### 匿名化・仮名化されたデータ

このグローバルポリシーは、完全に匿名である情報、すなわち、個人を特定できない情報には適用されません。今日の市場では、技術的なソリューションが利用できるため、適切な技術ツールを使用することで個人を特定するさまざまな方法があります。なお、匿名化の実現は実際には複雑である可能性があります。

このグローバルポリシーは、いわゆる偽名化された情報、すなわち別の情報（「鍵」など）を用いて個人と結びつけることができる情報にも適用されます。仮名化されたデータは、依然として個人データとみなされます。

**ノートです！**

個人データは、ゲティング社が保有するデータと、別のゲティング社または第三者が保有する他のデータとを組み合わせ、個人に関連付けることができる場合には、匿名化されているとはみなされません。例えば、静的 IP アドレスおよび動的 IP アドレスは、IP 番号がインターネット事業者の保有する情報と組み合わせられることにより、個人と関連づけることができるため、個人データに該当します。ゲティングが第三者の保有する情報にアクセスできなくても、すなわち個人データとみなされることは問題ではありません。

## 5. コンプライアンスに対する責任

### データプライバシーチーム

ゲティングのデータプライバシー組織とデータプライバシーチームは、データプライバシーガバナンス指令に記載されています。データプライバシーチームは、データプライバシーの分野において必要な専門的知識を保持するものとする。

データ・プライバシー・チームは、ゲティング社内のディスカッション・パートナーとみなされ、データ・プライバシーに関する問題では、データ・プライバシー・チームの意見が十分に尊重されるものとしします。

さらに見るデータ・プライバシー・ガバナンス指令

### ゲティング社各社の責任

このグローバルポリシーに記載されている法律、規制、ゲティング社内の決定、プロセス、手続きを遵守することは、各ゲティング社の最終責任となります。役割と責任については、第 19 項もご参照ください。

### リスクを報告する

ゲティングは、すべてのデータ保護法を完全に遵守し、違反につながる、またはその可能性のある業務慣行に積極的に対処し、是正するよう努めます。各従業員は、誠実に行動する者に報復やその他の否定的な結果がないことを保証された上で、コンプライアンス違反の事件や疑いを報告することが奨励され期待されています。従業員は、データプライバシーリスクおよび/または違反の疑いに関する懸念をデータプライバシーチームに提起することが期待されています。また、懸念は常に第 18 条に従って提起することができます。

## 6. ゲティング社がコントローラー（ ）または共同コントローラーとして個人データを処理する場合の一般要件

### コントローラー

ゲティングの会社が個人データを処理する場合、その理由と方法を決定し、独自の判断で処理することがあります。ゲティング社が個人データの処理の手段（方法）と目的（理由）を決定する場合、その企業はデータ管理者と呼ばれます。

**実施例**

ゲティンゲが毎月給与を支払う目的で従業員の個人データを収集する場合、ゲティンゲは処理の目的および手段を決定しているため、個人データの処理のデータ管理者とみなされます。

**ジョイントコントローラー**

特定の状況下では、2人以上のデータ管理者が、個人データの処理の目的（なぜ）と手段（どのように）を共同で決定することができます。例えば、ゲティンゲ社は、データ管理者の役割を1つまたは複数の社内および/または社外組織と共有することができます。これを「共同支配」といいます。

共同管理者の関係がある場合、データ管理者のそれぞれの責任を決定するために共同管理者契約を締結することが法的に義務付けられています。ゲティンゲ社は、イントラネットで利用可能な該当するテンプレートを確実に使用するものとします。

**実施例**

ゲティンゲ社が病院と共同で研究調査を行い、ゲティンゲ社と病院が共同で、プロジェクト内で個人データを処理する理由と方法を決定する場合、ゲティンゲ社と病院は共同管理者と見なされ、その場合、共同管理者契約を締結する必要があるものと思われれます。

**個人データの収集と処理に関する基本要件**

個人データは、特定された、明示的かつ正当な目的のためにのみ処理されるものとします。目的が正当であるとみなされるためには、データ対象者が処理に同意したか否かにかかわらず、計画された処理が必要です：

- a) 正当な事業目的を有し、データ保護法その他の法令に違反しないこと；
- b) 目的を達成するために比例して必要であること；
- c) データ対象者に不当な悪影響を及ぼす方法で使用されないこと。
- d) データ対象者の個人データは、データ対象者が合理的に期待する方法でのみ取り扱います。

個人データの処理はすべて、処理の目的を達成するために必要なものでなければならず、データ対象者は、個人データの処理の目的または範囲に関して、誤解や欺瞞を受けてはなりません。個人データは、データ対象者に通知された目的と相容れない方法で処理されることはありません。さらに、ゲティンゲ社が処理する個人データは正確であり、必要な場合には最新の状態に保つものものとします。

**個人データの処理に関する法的根拠****法的根拠に関する一般的な事項**

ゲティンゲは、以下の少なくとも1つに該当する場合にのみ、個人データを処理することができます：

- a) **同意する。** データ対象者が、特定された目的のために処理を行うことに事前に同意していること。同意および同意の撤回については、本条6項の下記をご参照ください。
- b) **法的義務を負う。** ゲティンゲは、ゲティンゲが従うべき法的義務（税務当局への所得税情報の提出など）を果たすために、個人データを処理する必要があります。

- c) **契約を履行すること。**個人データの処理は、ゲティンゲがデータ対象者と締結した契約における義務を果たすために必要です（雇用契約に基づいて給与を支払うために銀行口座の詳細を保持することなど）。
- d) **ゲティンゲの正当な利益**ゲティンゲは、データ主体の利益または基本的権利および自由によってかかる利益が優先される場合を除き、事業の一環としての正当な目的（顧客またはビジネスパートナーに関する情報のデータベース保持、従業員の緊急連絡先の名前および電話番号の収集など）のために個人データを処理することができます。この法的根拠が適用される場合、問題となる特定の利益を特定し、データ対象者にその旨を通知する必要があります。
- e) **その他個人データを処理することができるその他の稀な理由**は、データ対象者の重要な利益の保護または公共の利益のために実行される業務です。

### **同意 と同意の撤回**

同意は、他の法的根拠を用いることができない場合にのみ、ゲティンゲ社によって用いられるべきです。法的根拠として同意が適用される場合、ゲティンゲ社は、データ対象者が個人データの処理に同意したこと、および当該同意が有効であることを証明できなければなりません。事前にチェックされたボックス、沈黙、無活動は、決して同意とみなされません。適切な場合、処理の異なる目的について、個別の同意を得るべきである。

同意とする：

- a) 他の条件に左右されることなく与えられる；
- b) 情報提供される（データ対象者への情報提供については、本項の下記を参照）；
- c) 自発的に提供されること（データ対象者は同意を提供するよう圧力を感じてはならない）、および
- d) 具体的かつ曖昧でないこと（データ主体が同意の範囲を認識していること）。

同意は、書面または電子的に行われなければなりません。データ対象者が提案された個人データの処理を受け入れるかどうかは、明確に示されなければならない。同意は、沈黙や不活動によって提供されることはありません。

データ対象者は、提供された同意をいつでも撤回することができます。同意が撤回された場合、当該ゲティンゲ社は、同意に基づく処理の範囲内で、データ対象者に関する個人データの処理を停止するものとします。これは、同意を撤回した個人に関するすべての個人データを、バックアップの個人データも含めて、削除または匿名化する必要があることを意味します。

### **特別なカテゴリーの個人データを処理するための追加要件**

特別なカテゴリーの個人データは、しばしば「敏感な個人データ」と呼ばれ、特別な状況下でない限り、Getingeによって処理されることはありません。

特別カテゴリーの個人データの処理は、このセクション6で上述したように、処理に法的根拠がある場合にのみ実行することができます。また、当該データは、以下の条件のうち少なくとも1つが満たされた場合にのみ処理されることがあります：

- a) データ対象者が、指定された目的のために処理を行うことに明示的に同意していること；
- b) 国内法または労働協約で認められている限り、雇用法の分野におけるデータ管理者またはデータ主体の義務を遂行し、権利を行使する目的で処理が必要であること；
- c) 法的請求の確立、行使または防御のために処理が必要であること。
- d) 処理は、予防医学または産業医学の目的、従業員の労働能力の評価、医学的診断、健康管理または治療の提供のために必要です。

ゲティンゲは、通常、特別カテゴリーの個人データの処理を避けるべきであり、上記の1つ以上に該当する場合に限り、処理を行うことができます。また、地域によって例外が適用される場合があります。

**ノートです！**

明示的な同意は、同意および同意の撤回に関して本第6条に記載されているように、通常の同意の要件を含んでいます。また、本人は、提案された個人データの処理に同意するか否かの選択肢を明確に提示するものとします。

**犯罪歴・前科の範囲内の個人データ**

ゲティンゲは、適用される法律および規制によって許可または要求される場合を除き、疑いを含む犯罪歴または前科に関する個人データを処理しないものとします。なお、この種の個人データを処理することは、一般的に禁止されています。ただし、各国の法律や規制により免除される場合があります。

犯罪、前科または関連する疑いに関連する個人データを処理するために、ゲティンゲの異なる部門に要求がある場合があります。例えば、調査やデューデリジェンスにおいて、法務・コンプライアンス・ガバナンス部門が、企業や関連する役職の人物の事実確認や背景調査を行うことが（適用される法律や規制によってサポートされている場合）要求されることがあります。

**ノートです！**

犯罪歴、犯罪行為、前科、または関連する疑惑に関する個人データを処理する前に、データ・プライバシー・チームに必ず相談するものとします。

**データ対象者への情報提供**

Getinge は、データ対象者に対して、以下の情報を記載した書面を通知するものとします：

- a) データ管理者である事業者の名称および連絡先；
- b) 処理される個人データの種類および関連する処理の目的；
- c) プロセッシングの法的根拠
- d) 個人データの保存期間
- e) 個人データの受領者または受領者のカテゴリー；
- f) 以下のセクション8 に従ったデータ主体の権利に関する情報。
- g) 該当する場合：
  - i. の連絡先を担当のデータ保護責任者に連絡する；
  - ii. 個人データの取得先
  - iii. データ対象者が個人データを提供しない場合の結果；
  - iv. 以下のセクション9 に従い、個人データを EU/EEA 外に移転するゲティンゲの意図。
  - v. プロファイリングに関する情報です。

データプライバシーチームは、ゲティンゲ社が個人データの処理についてデータ対象者に通知する必要がある場合に、必ず使用しなければならないプライバシー通知のテンプレートを提供します。テンプレートには、データ対象者に提供しなければならない情報についての詳細な指示が含まれています。

プライバシーに関する告知が十分かつ完全であり、データ保護法を遵守していることを確認し、証明することは、ゲティンゲの各企業の責任である。さらに、ゲティンゲ社は、必要に応じて、プライバシー通知を現地語に翻訳するものとします。

従業員に関しては、個人データの処理に関する情報は、通常、従業員が雇用契約書とともに受け取る「従業員プライバシー通知」に記載されています。ゲティンゲの各企業は、従業員のプライバシーに関する通知を、従業員が容易にアクセスでき、最新のものであるとともに、会社が従業員に関する個人データをどのように処理するかについて十分な情報を提供するようにしなければなりません。

## 個人データの処理目的の変更

個人データの処理目的を変更する前に、ゲティンゲ社は以下を行うものとします：

- a) 個人データの処理の適法性を評価し、下記7項に従って評価を文書化すること；
- b) データ対象者に、処理の目的の修正を説明する書面を提供すること。
- c) 処理が同意に基づいている場合、データ対象者から新たな同意を得ること。

## プロファイリングと自動意思決定

### プロファイリング全般について

プロファイリングとは、データ対象者に関連する個人的側面を評価する、またはデータ対象者の仕事、経済状況、場所、健康、個人的な好み、興味、信頼性または行動、運転手の行動、顧客の行動、場所または移動を予測または分析する意図を含む、あらゆる形式の個人データの自動処理を指します。

プロファイリングは、様々なソースからのデータを用いて個人を予測し、統計的な推論を行うためによく用いられます。処理の目的は、データ対象者を特定のグループまたはカテゴリーに分類するために、データ対象者の特性または行動パターンを分析することである可能性があります。これにより、データ管理者は、データ対象者の興味、タスクの実行能力、または可能性のある行動などについて予測することができます。

### 実施例

プロファイリングとは、例えば、特定の製品やサービスに関するパーソナライズされた広告を送信するために、クッキー識別子や IP アドレスを通じてウェブサイト上での個人の行動を分析することを指します。また、過去に購入した商品を分析し、将来の購入を予測することもプロファイリングの一例です。したがって、プロファイリングは、ダイレクトマーケティングやソーシャルメディアに関連して一般的に使用される方法ですが、調査研究など他の処理活動にも使用される可能性があります。

### プロファイリングに基づく意思決定

プロファイリングに基づきゲティンゲ社が行う決定は、以下の場合にのみ許可されるものとします：



- a) データ主体とデータ管理者の間の契約の締結または履行のために絶対に必要な場合（この例外は狭く解釈されるべきです）；
- b) 機関や国の監督機関の規制、基準、勧告に従って実施される詐欺や脱税の監視・防止目的、およびゲティングが提供するサービスのセキュリティと信頼性を確保するためなど、法律で明示的に許可されている場合、または
- c) データ対象者が明示的に同意した場合。

### 必要条件

ゲティング社は、プロファイリングに従事する際、以下のことを確認するものとします：

- a) 目的を達成するために必要な個人情報のみを処理すること；
- b) 第6条に従って、データ対象者にプロファイリングに関する十分な情報を提供すること。プロファイリングが自動的な意思決定に関するものである場合、データ対象者は、到達した意思決定に関する説明、および当該意思決定に異議を申し立てる権利に関する情報を得る権利を有します；
- c) プロファイリングに適切な数学的または統計的手順を使用すること；
- d) 0 に従い、適切な技術的および組織的対策を実施する。
- e) データ主体の権利と利益に関わる潜在的なリスクを考慮し、特に、特別なカテゴリーの個人データに基づく個人に対する差別的な効果、またはそのような効果を持つ措置をもたらすことを防止する方法で、個人データを保護すること。

#### ノートです！

プロファイリングは、実施前にデータ・プライバシー・チームの事前承認を得るものとする。

### 個人データの保持・保管・削除について

ゲティング社は、個人データがそれ以上長く処理されないようにするものとします：

- a) 処理の目的との関係で必要であること。
- b) データ保護法により許可されています。

ゲティング社は、このセクションの要件が満たされるように処理を実施するものとする。

#### ノートです！

一部の国（ロシアや中国など）では、国民に関するすべての個人データをその国の国境内で保存することを義務付けています。他の国では、特定の目的のために処理される場合、特定の個人データを現地で保管することが要求される場合があります（例：スウェーデンでは会計情報を国境内で保管することが要求されています）。ローカライゼーション要件は、通常、ゲティングが個人データのコピーを他の場所にも保存することを妨げるものではなく、そのような保存が必要な場合は、そのようにします。

## 7. Processing の評価と文書化

### 加工活動の記録

データ保護法により要求された場合、ゲティンゲの各社は、各社の処理活動の記録を残す責任があります。すべての記録は、選択したコンプライアンスツールで管理し、データ・プライバシー・チームが取り扱うものとする。詳細は、「データ・プライバシー」のイントラネットページでご確認ください。

このセクションの要件は、ゲティンゲ社がデータ管理者及びデータ処理者として行動する場合の両方に適用されます。

### 新たな加工活動を開始する前の合法性の評価

新しい処理活動を行う前、または進行中の活動に変更を加える前に、ゲティンゲ社は個人データの処理の合法性を評価し、その評価を文書化するものとします。これは、これまで評価および/または文書化されていなかった、進行中の処理活動にも適用されます。

このセクションの要件は、ゲティンゲ社がデータ管理者及びデータ処理者として行動する場合の両方に適用されます。

### データ保護影響評価 (Data Protection Impact Assessments)

個人データの処理がデータ主体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、Getinge 社は、そのような想定される処理が開始される前に、処理業務が個人データの保護に及ぼす影響の評価（データ保護影響評価）を行うものとします。データ保護影響評価は、特に、Getinge 社が新しい技術を使用し、処理の性質、範囲、文脈、目的を考慮する場合に関連することがあります。

データ保護影響評価は、常にデータプライバシーチームがゲティンゲ社に代わって実施するものとします。ゲティンゲ社は、評価の過程で、必要な情報を提供するなど、データ・プライバシー・チームに協力するものとします。

## 8. データ主体の権利

### データ主体の要求への対応

データ主体からの要請については、以下のとおりです：

- a) データ対象者からのすべての要求は、データ・プライバシー・チームに直ちに転送され、処理されるものとします。
- b) データ対象者は、データ対象者の権利を行使する際に、否定的な結果に直面することはない。
- c) すべてのデータ対象者の要求は、秘密厳守で処理されるものとします。
- d) ゲティンゲ社は、データ・プライバシー・チームがタイムリーに要求に答えることができるように、データ・プライバシー・チームに協力するものとします。

データ主体の権利は絶対的なものではなく、例外が適用される場合があることに注意する。

## データ主体の権利を処理するためのプロセス

ゲティンゲ社は、データプライバシーチームによるデータ主体の権利の取り扱いを支援するためのプロセスを導入する責任があります：

- a) 個人データへのアクセスを要求する。これには、データ対象者が当該個人に関連する個人データの処理に関する情報を受け取る権利、およびデータポータビリティの権利を確保することが含まれます。
- b) 不正確な個人データの訂正を要求すること。
- c) 個人データの消去を請求する。
- d) 個人情報の処理がゲティンゲの正当な利益に基づいている場合、その処理がプロファイリングに関係する場合を含め、いつでも異議を申し立てることができます。
- e) 個人データの制限を受けること。

## 9. 個人データの譲渡について

### 乗り継ぎに関する一般的なこと

個人データは、処理の目的を達成するためにのみ移転されるものとしします。なお、個人データの転送とは、電子メール等の電子的メッセージによる個人データの送信だけでなく、個人データへのアクセスや閲覧が可能な場合も含まれます。個人データは、一時的にアクセス、閲覧、またはその他の処理が行われただけでも、転送されたとみなされます。

#### 実施例

フランスのゲティンゲ社が個人データをフォルダに保存し、中国のゲティンゲ社の従業員がアクセスできるようにした場合、個人データが転送されます（EU/EEA から EU/EEA 以外の国への個人データの転送に関しては、このセクション9も参照してください）。

### EU/EEA から EU/EEA 以外の国への個人データの移転について

EU/EEA 内のゲティンゲ社は、原則として個人データを EU/EEA 外に転送しないものとしします。このような転送は、厳密に必要な場合にのみ行われます。

EU/EEA 内の国から EU/EEA 外の国への個人データの転送が厳密に必要な場合、Getinge 社は以下を確実に行うものとしします：

- a) かかる移転は、データ保護法に基づく適切な保護措置に従うものとする（これらに限定されない）：
  - i. 欧州委員会が行う妥当性判断のこと；
  - ii. 欧州委員会が採択した EU 標準契約条項、または
  - iii. 明示的な同意。
- b) 必要であれば、トランスファーインパクトアセスメントも行っています。

個人データの移転に先立ち、データ対象者は、第6条に基づき、移転および適用される適切な保護措置に関する情報を受領する権利を有します。

## 10. ゲティング社内での個人データの共有と開示

ゲティングの従業員およびコンサルタントは、業務遂行のために当該データを必要とするゲティング社内の個人、および当該個人データを共有または開示する正当な業務目的がある場合に限り、個人データを共有および開示します。個人データは、処理の目的を達成するために必要な範囲でのみ、共有または開示されることがあります。個人データは、受け取る側にとって「あったらいいな」という理由で共有または開示されることはありません。

## 11. データ処理業者

### 契約書の条項に関する一般的なこと

必要に応じて、個人データ処理条項および/またはデータ処理契約を、ゲティングの標準的なビジネス契約および雇用契約に含めることは、ゲティングの会社の責任となります。

既存の契約が既に締結されている場合、ゲティング社は、個人データ処理条項および/または関連するデータ処理契約により、必要に応じて当該契約を更新するものとします。

#### ノートです！

データ処理契約が必要な場合は、データプライバシー・イントラネットのページで公開されているデータ処理契約テンプレートを常に使用する必要があります。

### 第三者との関係におけるデータ処理者としてのゲティング社

ゲティングの会社が第三者（顧客など）に代わって個人データを処理する場合、ゲティングと第三者はデータ処理契約を締結するものとします。ゲティング社は、イントラネットで利用可能な該当するテンプレートを確実に使用するものとします。

#### 実施例

ゲティングは、ほとんどの場合、病院への当社のソフトウェアソリューションの提供に関連して、データ処理者として行動します。これは、当社がソフトウェアサポートを提供する際に、ゲティングが個人データにアクセスする必要がある場合、またはその他の方法で個人データを処理する必要がある場合です。これらの状況に対して、当院はデータ管理者として行動します。

### 外部のデータ処理業者と契約する

第三者がゲティングに代わって個人データを処理する場合（サプライヤーなど）、ゲティングと第三者はデータ処理契約を締結するものとします。ゲティング社は、イントラネットで利用可能な該当するテンプレートを確実に使用するものとします。

#### 実施例

ゲティングが新しい IT システム/ソリューションを購入し、その IT システム/ソリューションのサプライヤーがゲティングに代わって個人データを処理すること（個人データの保存や、サポートを提供する際の個人データへのアクセスなど）を含む場合、ゲティングとサプライヤー

は、データ処理契約を締結するものとします。この場合、Getinge はデータ管理者であり、供給者はデータ処理者です。

### 他のゲティンゲ社に関連するデータ処理者としてのゲティンゲ社

ゲティンゲ社が他のゲティンゲ社を代表して個人データを処理する場合、当事者はグループ内データ処理契約を締結するものとします。ゲティンゲの各社/各機能は、以下のことを確実に行うものとする：

- a) データ・プライバシーに関するイントラネットのページで入手できる該当するテンプレートを使用する。
- b) グループ内データ処理契約が既に締結されていること。

#### 実施例

Getinge IT が Geting HR に代わって個人データを処理することを含むサポートで Geting HR を支援する場合、グループ内データ処理契約を締結するものとします。この場合、Getinge IT はデータ処理者であり、Getinge HR はデータ管理者です。

## 12. 技術的・組織的なセキュリティ対策

すべてのゲティンゲ社は、情報セキュリティに関するゲティンゲ社の方針および指令に従うものとします。また、ゲティンゲ社は、リスクに見合ったセキュリティレベルを確保するために、適切な技術的・組織的対策を実施するものとします。このような措置を講じる場合には、以下の点に留意する必要があります：

- a) の状態です；
- b) 導入にかかる費用です；
- c) 処理の性質、範囲、目的、および
- d) データ対象者の権利と自由に対する可能性と重大性のリスク。

個人データの処理がデータ保護法に準拠していることを確認することは、アクセス権、削除のための個人データのフラグ立て、自動削除、データの記録など、適切な技術的および組織的措置を講じることを含め、各ゲティンゲ社の責任となります。アクセス権に関して、ゲティンゲ社は、ゲティンゲ社内での役割が変更された場合を含め、個人データへのアクセスが従業員およびコンサルタントの役割を反映するようにするものとします。

## 13. IT ソリューション 個人データの処理

個人データを処理するために使用される新規および既存の IT 機能、ソリューションおよび/またはサービスが、以下の要件を含むがこれに限定されないデータ保護法に準拠していることを確認することは、各ゲティンゲ社の責任である：

- a) デザインによるプライバシーとデフォルトによるプライバシー；
- b) データの保持；
- c) データポータビリティを含む、データ主体の要求；

- d) 技術的・組織的なセキュリティ対策が十分であること。
- e) アクセス権です。

新しい IT ソリューションが使用される前、および既存の IT ソリューションに変更が加えられる前に、ゲティンゲ社は、プライバシーリスク、目的、処理される個人データについて、適時にデータプライバシーチームに報告するものとします。また、既存の IT ソリューションにおける個人データの処理についても、データ・プライバシー・チームに情報を提供するものとする。

さらに見る情報セキュリティ指令

## 14. デザインおよびデフォルトによるプライバシー

ゲティンゲが個人データの処理を含むアプリケーション、サービス、製品を開発、設計、選択、使用する際には、設計によるプライバシーとデフォルトによるプライバシーの原則が考慮されるべきです。これらの原則は、処理の手段を決定する時点と処理そのものを行う時点の両方で実施されるべきです。

プライバシー・バイ・デザインとは、エンジニアリングのプロセスを通じてデータ保護を考慮するシステム工学の概念およびアプローチです。プライバシー・バイ・デザインは、プライバシーが情報技術、ビジネスプロセス、物理的空間、ネットワークインフラに最初から組み込まれていることを保証することに焦点を当てます。

ゲティンゲは、自社のシステムやプロセスが特にデータ保護を念頭に置いて設計されていることを確認する必要があります。データ保護は後付けではなく、企業がビジネスを遂行するための基盤に組み込まれるべきです。

既定によるプライバシーとは、データ管理者が、既定により、必要な個人データのみが処理の特定の目的ごとに処理され、特に、データ量および保存時間の両面において、その目的に必要な範囲を超える収集または保持が行われないようにするための仕組みを導入することをいいます。特に、実施されたメカニズムは、デフォルトで個人データが不特定多数の個人にアクセスできるようにならないことを保証するものとする。

### 実施例

例として、ゲティンゲが個人データを保存またはアクセスするための新しい IT システムを構築し、データプライバシーに影響を与えるポリシーまたは戦略を策定し、個人データの共有または新しい目的での使用を開始する場合、デザインおよびデフォルトによるプライバシーを考慮することが適切であるでしょう。

プライバシー・バイ・デザインおよびデフォルトを念頭に置いて、プロジェクト、プロセス、製品、またはシステムを当初から設計することは、以下のような利点があります：

- a) 潜在的な問題を早期に発見することができ、その対処はよりシンプルで低コストとなることが多い；
- b) 組織全体のデータプライバシーに対する意識が高まります；
- c) データ保護法の義務を果たす可能性が高まり、同様に違反の可能性が減少します。
- d) プロジェクト、プロセス、製品またはシステムは、プライバシーを侵害する可能性が低く、個人に悪影響を与える可能性があります。

特に、個人データに関連する製品やサービスをゲティンゲが設計・開発する場合、ゲティンゲがどのようにプライバシー・バイ・デザインおよびバイ・デフォルトの要件に準拠すべきかという関連する詳細を定義する必要があります。

## 15. 個人情報漏えいについて

すべての個人情報漏洩は、データ・プライバシー イン트라ネットのページに記載されているプロセスに従って、直ちに報告されるものとします。

Getinge 社のものとする：

- a) 個人データの処理に使用されるすべてのソリューションが、個人データ侵害の報告を可能にすることを保証する；
- b) 個人情報漏えいの検出を支援する措置を講じること；
- c) 個人データ漏洩の状況（影響、考えられるリスク、実施または計画された救済策を含む）を記録すること。
- d) 個人データの侵害が調査され、改善された場合、データ・プライバシー・チームに協力すること。

さらに見る個人情報漏洩防止指令

## 16. 監督官庁

監督官庁との連絡は、すべてデータ・プライバシー・チームが行うものとする。ゲティンゲ社は、要請に応じて監督官庁に協力するものとします。

## 17. 偏差値

このグローバルポリシーからの逸脱は、グローバルポリシーが最初に承認されたときと同じレベルの権限で承認されるものとします。

## 18. グローバルポリシーに対する違反行為 - Speak Up

遠慮せずに悩みを打ち明けてください。このグローバルポリシーの違反が疑われるゲティンゲの社員は、ラインマネージャー、倫理・コンプライアンスオフィス、またはゲティンゲ・スピークアップ・ラインを利用して、問題を提起することが期待されます。Getinge Speak Up Line は、Getinge の社内外のウェブページで利用できます。ゲティンゲでは、懸念や意見を表明した人に対するいかなる報復も認めません。

さらに見るグローバルスピークアップと報復禁止指令

## 19. 役割との責任

ゲティンゲの全社員は、このグローバルポリシーを読み、理解し、遵守する責任を個別に負っています。社員一人ひとりが、このグローバルポリシーに則って行動する責任を負っています。

各ラインマネージャーは、各チームメンバーがこのグローバルポリシーと関連する指令、指示、ガイドラインにアクセスできることを確認する責任があります。

データプライバシーに関する定期的な情報提供やトレーニング、コンプライアンスのフォローアップなど、日常的な強化はすべてのマネージャーの責任です。

このグローバルポリシーに違反した場合、解雇を含む懲戒処分の対象となります。

## 20. ガイダンスとアシスト

データ・プライバシーの分野におけるゲティンゲの立場について、私たちの行動を導くために、このグローバル・ポリシーといくつかの指令や指示があります。本グローバルポリシーについてご質問がある場合、またはどのルールが適用されるか不明な場合は、データプライバシーチームまでご連絡ください。

## 21. お役立ちリンク集

### タイトル

---

個人情報漏えい指令

---

データプライバシーガバナンス指令

---

情報セキュリティ指令

---

グローバルスピークアップ・非報復指令

---