データ処理契約

https://scratcher.io/ja/data-processing-agreement

標準版、最終更新日：2026年10月22日。本データ処理合意書は、お客様がScratcherをご利用になる際の、お客様とScratcher ApS（CVR 38552864, Fruebjergvej 3, 2100 Copenhagen Ø,
Denmark）との間の契約の一部を構成するものです。本合意書は、GDPR第28条の要件を満たすよう作成されています。

データ処理合意書

本データ処理合意書は、カスタマーとScratcherとの間の契約の不可分の一部を構成します。本データ処理合意書が本契約に添付されている場合、利用規約第10条は適用されず、本データ処理合意書が適用されるものとします。

1. 定義

1.1.

文脈上別段の明示的な定めがない限り、本データ処理合意書における以下の定義語は、以下の意味を有するものとします。

- 「データ侵害」とは、処理される個人データの偶発的若しくは不法な破壊、紛失、改ざん、権限のない開示（無許可での開示）、又はアクセスをもたらす、個人データのセキュリティに対する偶発的若しくは不法な侵害を意味します。
- 「データ管理者」とは、GDPRに定義される個人データの処理の目的及び手段を決定するカスタマーを意味します。
- 「データ処理者」とは、データ管理者に代わって個人データの処理に従事するScratcherを意味します。
- 「個人データ」とは、データ処理者が本契約に基づきデータ管理者に代わって処理する、特定された又は特定可能な自然人に関するあらゆる情報（GDPR第4条第1号）を意味します。
- 「GDPR」とは、個人データの処理に係る自然人の保護及び当該データの自由な移動に関する、並びに指令95/46/ECを廃止する2016年4月27日の欧州議会及び理事会規則(EU) 2016/679（一般データ保護規則）を意味します。
- 「復処理者」とは、データ処理者の従業員を除き、データ処理者に代わって、かつ本データ処理合意書に指定された範囲及び目的のためにその指示に従い個人データを処理するために、データ処理者によって委託された者を意味します。

1.2.

上記で定義されていない大文字で始まる用語は、文脈上別段の明示的な定めがない限り、本契約で定義されている意味と同じ意味を有するものとします。

2. 適用範囲

2.1.

本データ処理合意書に含まれる条件は、データ管理者の代行として、かつその指示に基づいてデータ処理者が行なう個人デ

ータの処理に適用されます。

2.2.

本データ処理合意書においてデータ処理者に言及している場合、本データ処理合意書の関連規定は、データ処理者が委託する復処理者にも適用されるものとします。

3. データ管理者の指示及び処理条件

3.1.

データ処理者は、データ処理者が従うべきEU若しくは加盟国の法律により義務付けられている場合を除き、第三国への個人データの移転に関するものを含め、データ管理者の文書による指示に従ってのみ個人データを処理するものとします。そのような場合、データ処理者は、当該法律が公共の利益に関する重大な理由によりかかる通知を禁止していない限り、処理を行う前にその法的要件についてデータ管理者に通知するものとします。

3.2.

データ処理者は、データ管理者（その顧客を含みます）が本サービスを利用する際にアップロード又は送信するデータ主体のカテゴリーの個人データを処理するものとします。データ管理者に代わって処理される個人データの種類及びデータ主体のカテゴリーは、本データ処理合意書の付録Aに記載されています。

3.3.

両当事者は、本データ処理合意書及びデータ管理者が本サービスを利用する際に成立する契約を、データ管理者の文書による指示とみなすことに合意します。データ管理者は、本サービスの設定を調整することにより、個人データの収集に関する追加の文書による指示をデータ処理者に提供することができます。また、両当事者は、データ管理者の追加の指示の実行及びその費用について書面で合意することができます。

3.4.

データ処理者は、データ管理者が本サービスの利用時に個人データをアップロード又は送信した時点からそれが削除されるまで個人データを処理するものとします。ただし、本データ処理合意書第12条に規定する期間を超えないものとします。

3.5.

データ処理者は、ある指示がGDPR又はその他のEU若しくは加盟国のデータ保護規定に違反すると判断した場合は、直ちにデータ管理者に通知するものとします。

3.6.

データ管理者は、データ処理者の要請に応じ、データ処理者がデータ管理者に代わって個人データを処理する際にGDPRのすべての要件を適切に遵守するために必要な情報、文書、又は支援を遅滞なく提供することを約します。

4. 個人データの秘密保持

4.1.

データ処理者は、本サービスの提供及び本契約に基づく権利の行使の目的にのみ個人データを使用するものとします。法律により別段の定めがある場合を除き、データ処理者は個人データを第三者に開示してはなりません。

4.2.

データ処理者は、業務の遂行又はデータ処理者へのサービスの提供のために当該データを必要とするデータ処理者の従業員又はサプライヤーにのみ個人データへのアクセスが許可されること、及び個人データの処理を許可されたすべての者が秘密保持義務を約しているか、又は適切な法的秘密保持義務を負っていることを確保するものとします。

4.3.

データ処理者が法令の要件を遵守するために個人データを第三者（例：法執行星官等）に開示する義務を負う場合、データ処理者は、法令により別段の定めがある場合を除き、個人データの開示要件について直ちにデータ管理者に通知するものとします。

4.4. これらの秘密保持義務は、本データ処理合意書の終了後も有効に存続するものとします。

5. 技術的及び組織的措置

5.1.

データ処理者は、最新技術、導入費用、処理の性質、範囲、文脈及び目的、ならびに自然人の権利及び自由に対する発生確率と重大性が多様なリスクを考慮し、個人データの処理前及び個人データの処理中のいかなる時点においても、個人データのセキュリティを確保するために必要な適切な技術的及び組織的措置を実施するものとします。適切なセキュリティレベルを確保するための技術的及び組織的措置を選択及び実施するにあたり、データ処理者は、データ主体の個人データの処理、送信、保管又はその他の方法で処理されたデータの偶発的若しくは不法な破壊、紛失、改ざん、無権限の開示若しくは不法なアクセスから生じるリスクを特に考慮するものとします。

5.2.

データ処理者はその分野の専門家であり、本サービスの提供に関する知識と経験を有しているため、本データ処理合意書第5.1条に記載された目的を達成するために必要な技術的及び組織的措置を選択及び決定するものとしますが、かかる措置は、いかなる場合においても適用法令の要件を遵守するものとします。それにもかかわらず、データ管理者は、技術的及び組織的セキュリティ措置の適用に関してデータ処理者に指示及び提案を与える権利を有するものとします。データ処理者は、データ管理者からのそのような提案を考慮し、検討した上で、(i)
データ管理者の指示をどのように実施するかについて理由を付した回答をデータ管理者に提供し、(ii)
かかる措置を実施するための即座の対応をとるものとします。

5.3.

本データ処理合意書の締結時点でデータ処理者が実施している技術的及び組織的措置は、付録Cに記載されています。データ処理者は、ISO/IEC

27001の認証を受けた情報セキュリティマネジメントシステムを維持しており、全体的なセキュリティレベルが低下しないことを条件として、時間の経過とともに措置を更新することがあります。

5.4.

処理の性質及び自らが利用可能な情報を考慮し、データ処理者は、GDPR第32条に基づく義務の遵守を確保するにあたり、データ管理者を支援するものとします。

6. データ処理の監査

6.1. データ処理者は、現在のISO/IEC

27001認証書、及び要請に応じて適用宣言書を含め、GDPR第28条に定められた義務の遵守を証明するために必要なすべての情報をデータ管理者が利用できるようにするものとします。

6.2.

データ処理者が個人データを適切に処理しているかどうかを検証するため、データ管理者は、以下の条件の下で当該処理の検査を実施する権利を有するものとします。(i) 監査は個人データの処理のみに関連すること、(ii)

データ管理者は、監査の実施希望を4週間を下回らない合理的な期間内にデータ処理者に通知しなければならないこと、(iii)

監査はデータ処理者の日常の業務活動を妨げない方法で実施されなければならないこと、(iv)

監査はデータ管理者の費用で実施されなければならないこと、(v)

監査は、その候補者がデータ処理者によって事前に承認された独立した人物（当該承認は不当に保留されないものとします）によって実施され、かつ当該人物はデータ処理者の秘密情報を保護することを約さなければならないこと。

6.3.

データ処理者は、監査の実施における支援に対して報酬を受け取る権利を有するものとします。当該報酬の額は、監査に関連してデータ処理者が負担した費用を考慮してデータ処理者が決定するものとします。データ処理者は、監査の前に報酬の額をデータ管理者に通知するものとします。

6.4. 管轄の監督機関によって実施される監査及び検査には、第6.2条及び第6.3条の条件は適用されません。

6.5.

監査の結果にデータ管理者が満足しない場合、データ管理者は、裁判外の手続きにより、本データ処理合意書及び本契約を一方的に解約する権利を有するものとします。この場合、本契約の解約はデータ管理者が講じることができる唯一の措置であり、データ処理者はデータ管理者に対していかなる損害も賠償する義務を負わないものとします。

7. 復処理者

7.1.

データ管理者は、本データ処理合意書に指定された範囲及び目的内で、データ処理者に代わって個人データを処理する復処理者を委託することについて、ここにデータ処理者に対して一般的な事前同意を与えるものとします。

7.2.

データ処理者は、委託された復処理者との間で書面による合意が締結されていることを確保するものとし、それにより復処理者は、本データ処理合意書に定められたものと同じデータ保護義務を遵守すること、特に処理がGDPRの要件を満たすような方法で適切な技術的及び組織的措置を実施するための十分な保証を提供することを約するものとします。データ処理者は、復処理者の義務の履行についてデータ管理者に対して責任を負うものとします。

7.3.

復処理者の現在のリストは、本データ処理合意書の付録Bに記載されています。データ処理者は、復処理者を変更又は新規に委託する計画について、予定されている事象の遅くとも14カレンダー日前までにデータ管理者が当該情報を利用できるようにすることにより、データ管理者に通知するものとします。

7.4.

データ処理者が本データ処理合意書第7.3条に規定する手続きに従って通知を行った後、復処理者の変更又は新規委託に続いてデータ管理者が本サービスの利用を継続した場合、データ管理者はデータ処理者によるかかる行為に同意したものとみなされます。データ管理者が復処理者の変更又は委託に同意しない場合、データ管理者は裁判外の手続きにより一方的に本契約を解約する権利を有するものとします。その場合、本契約の解約はデータ管理者が講じることができる唯一の措置であり、データ処理者はデータ管理者に対していかなる損害も賠償する義務を負わないものとします。

7.5.

データ管理者が復処理者を委託することに対する一般的な同意を撤回した場合、データ処理者は裁判外の手続きにより一方的に本契約を解約する権利を有し、かかる解約は重要な理由により行われたものとみなされ、データ管理者は当該解約の結果としていかなる損害も被らなかったものとみなされます。

8. データ侵害

8.1.

データ処理者は、個人データに影響を与えるデータ侵害について知った後、不当な遅滞なく、ただし24時間以内に、営業提案書に記載された電子メールアドレス、記載がない場合はデータ管理者のアカウント所有者の電子メールアドレス宛てにデータ管理者に通知するものとし、提供される本サービスの性質及び個人データの処理ならびに利用可能な情報を考慮した上で、以下の情報をデータ管理者に提供するものとします。(i)
可能である場合はデータ主体のカテゴリー及びその概数を含むデータ侵害の性質、(ii)
データ侵害から生じる可能性のある結果、(iii)
データ侵害に対応するためにデータ処理者が実施した又は提案する措置（該当する場合は、データ侵害による不利益な結果を軽減するための措置を含む）、(iv) データ保護責任者又は詳細情報を提供できるその他の連絡担当者の氏名及び連絡先。

8.2.

データ処理者は、データ侵害に関する事実、その影響及び講じた是正措置を含め、すべてのデータ侵害を記録するものとし

ます。GDPR又はその他の適用法令で規定されている場合、データ処理者は当該記録を監督機関に提供するものとします。

8.3.

処理の性質及び自らが利用可能な情報を考慮し、データ処理者は、GDPR第33条及び第34条に基づく義務の遵守を確保するにあたり、データ管理者を支援するものとします。監督機関及び必要な場合はデータ主体への通知責任は、引き続きデータ管理者が負うものとします。データ侵害が本データ処理合意書に基づくデータ処理者の義務の違反によって引き起こされた場合を除き、第8.1条の通知を超えるデータ処理者の支援には追加費用が発生する場合があります。

9. 第三国への個人データの移転

9.1.

データ処理者による第三国（EU/EEA域外）への個人データの移転は、データ管理者からの文書による指示に基づいてのみ行われるものとし、常にGDPR第V章に従うものとします。

9.2.

データ管理者による付録Bに記載された復処理者の承認は、そこに記載されている通り、それらの復処理者が行う移転についての文書による指示を構成します。そのような各移転は、欧州委員会の十分性認定（認証された受領者のためのEU–US Data Privacy
Frameworkを含む）、欧州委員会の標準契約条項、又はGDPR第V章に基づくその他の移転ツールに基づくものとします。

10. 協力

10.1.

提供される本サービスの性質及びカスタマーデータの処理ならびに利用可能な情報を考慮し、データ処理者は、GDPR第32条～第36条に指定された義務の履行を確保するためにデータ管理者に協力するものとします。この目的のために、かつ本データ処理合意書に指定された範囲内に限り、データ処理者は、GDPRに基づくデータ管理者の義務の適切な履行に必要な要請された情報をデータ管理者に提供するものとします。

10.2.

特に新しい技術を使用する処理の種類が、処理の性質、範囲、文脈及び目的を考慮して、自然人の権利及び自由に対する高いリスクをもたらす可能性が高い場合、データ処理者は、処理を行う前に、想定される処理作業が個人データの保護に与える影響の評価の実施においてデータ管理者を支援するものとします。

10.3.

データ主体、監督機関、又は第三者が法令に基づきデータ処理者に対し、処理された個人データに関する情報の提供を要請した場合、データ処理者は不当な遅滞なくかかる要請をデータ管理者に転送するものとします。データ処理者は、データ主体、監督機関、又は第三者の要請への対応、及び個人データの訂正及び消去の権利、データポータビリティの権利、処理に対する異議申し立て及び制限の権利を含むがこれらに限定されないデータ主体の権利の実現に関連するデータ管理者の義務

の履行において、必要な範囲でデータ管理者を支援することを約します。データ処理者は、自らが保有する情報が法律で定められた期限内に伝達されることを確保するものとします。

11. データ管理者の義務

11.1.

データ管理者は、その単独の裁量と責任において、データ処理者に提供される個人データの種類及びデータ主体のカテゴリーを決定し、データ処理者による本サービスの適切な提供に必要な個人データのみをデータ処理者に提供するものとします。データ管理者は、データ処理者が不要な個人データを受領するリスクを含め、伴うすべてのリスクを負うものとします。

11.2.

データ管理者は、データ処理者に個人データを提供し、かつ本契約に基づいて個人データを処理するようデータ処理者に委託するために必要なすべての許認可及び承認を取得し、本契約の期間を通じてこれを維持することを表明し、保証します。

12. 個人データの消去及び返還

12.1.

本契約又は本データ処理合意書の終了時、データ処理者は、データ管理者の選択に基づき、データ管理者に代わって処理されたすべての個人データを消去するか、又はすべての個人データをデータ管理者に返還し（データ管理者は本サービスからいつでもデータをエクスポートできます）、既存のコピーを消去し、それを完了したことをデータ管理者に証明するものとします。ただし、EU若しくは加盟国の法律が個人データの保持を義務付けている場合を除きます。バックアップ内のコピーは、通常のサイクルでバックアップの期限が切れると消去され、その間は他の目的には使用されません。

13. 責任

13.1.

データ管理者が被ったいかなる損害にかかわらず、本データ処理合意書に基づくデータ処理者の全責任は、以下のように制限されるものとします。本データ処理合意書に起因又は関連して発生するあらゆる請求に対するデータ処理者及びそのサプライヤーの損害賠償責任の総額は、請求の原因となった事象の日から遡る12か月間にデータ管理者が本サービスに対してデータ処理者に実際に支払った額を超えないものとします。適用法令により認められる最大限において、データ処理者又はそのサプライヤーは、特別損害、附随的損害、間接損害、又は派生的損害（利益、データ、若しくはその他の情報の喪失、事業の中断、人身傷害、プライバシーの喪失による損害を含みますがこれらに限定されません）について、データ処理者又はサプライヤーがかかる損害の可能性について助言を受けていた場合であっても、また救済措置がその本質的目的を達しない場合であっても、一切の責任を負わないものとします。

13.2.

第13.1条の制限は、当事者間でのみ適用されます。適用法令に基づき制限できない責任には適用されず、GDPR第82条に基づくデータ主体の権利には影響を与えません。

14. 有効期間及び解約

14.1.

本データ処理合意書は、本契約の効力発生時に効力を生じ、本契約が効力を有する限り有効に存続するものとします。データ処理者の義務は、データ管理者に代わって個人データを処理する限り継続します。

15. 最終規定

15.1.

データ処理者は、データ処理合意書に対する変更の予定について、変更予定日の少なくとも30日前に通知するものとします。データ処理合意書の変更の発表後にデータ管理者が本サービスの利用を継続した場合、データ管理者はデータ処理合意書の変更に同意したものとみなされます。データ管理者が変更に同意しない場合、データ管理者は本サービスを利用できなくなり、本契約を解約する権利を有するものとします。

15.2.

本データ処理合意書と本契約との間に不一致がある場合、個人データの処理に関しては本データ処理合意書が優先するものとします。

15.3.

本データ処理合意書は、本契約に規定されているのと同じ法律に準拠し、紛争も同様の方法で解決されるものとします。

15.4. 付録：

- 付録A：個人データの処理に関する詳細
- 付録B：承認された復処理者
- 付録C：技術的及び組織的措置

付録A – 個人データの処理に関する詳細

対象事項及び期間	本契約の期間中の本サービスに関連する個人データの処理、及びその後第12条に基づき個人データが消去又は返還されるまでの処理。

処理の性質	ホスティング及び保管、データ管理者のキャンペーン及びフォームを通じた個人データの収集、本サービス内での表示、エクスポート及び消去、データ管理者が設定した参加者への電子メール及びメッセージの送信（例：確認、コード、賞品通知）、データ管理者の指示に基づく連携、Webhook及びAPIを通じたデータ管理者自身のシステムへの転送、サポート及びエラー処理。
個人データ処理の目的	本契約で合意された通り、データ管理者がデータ処理者の本サービスを利用できるようにすること
個人データ処理作業	本サービスの利用中に提供された個人データを含むカスタマーデータの収集及び保管
個人データの種類	名、姓、メールアドレス、IPアドレス及びそこから導き出される大まかな位置情報、登録日時（作成日時）、ならびに誕生日や電話番号などの追加データ（カスタマーが収集した場合）。データ管理者のキャンペーン設定に応じて、キャンペーンの質問への回答、ゲーム結果及び獲得した賞品、コード、同意記録、参加者がアップロードしたファイル（画像など）、ブラウザやデバイス情報などの技術データ。
データの特別なカテゴリー	対象外。データ管理者は、書面で合意されない限り、本サービスを通じて特別なカテゴリーの個人データ（GDPR第9条）又は有罪判決に関するデータ（GDPR第10条）を収集しないものとします。
データ主体のカテゴリー	データ管理者（カスタマー）のキャンペーンの参加者、登録を行わないデータ管理者のキャンペーンの訪問者（IPアドレス、大まかな位置情報、ブラウザ情報）、及びデータ管理者に代わってデータが処理される範囲でのデータ管理者の本サービスユーザー。
個人データの処理場所	個人データは、データ処理者の施設内、及び欧州連合内に位置する仮想サーバー上、ならびに付録Bに記載されている復処理者によって同付録に記載された場所で処理されるものとします。
処理の期間/保管期間	データ管理者が本サービス内で設定した期間。利用規約第9.4条に従い、データ処理者は3年を超えて経過した個人データを消去する場合があります。

付録B – 承認された復処理者

データ処理合意書の締結時点で、データ管理者は以下に記載する復処理者の委託を承認します。EU/EEA域外への移転は、受領者が認証を受けている場合はEU–US Data Privacy Frameworkに、又は欧州委員会の標準契約条項（第9.2条）に基づくものとします。

復処理者	処理の概要	処理の場所
Amazon Web Services EMEA SARL, Luxembourg (AWS)	本サービスのホスティング：サーバー、データベース、ファイルストレージ、バックアップ、キャッシュ、ログ	欧州連合（スウェーデン、ストックホルム）。コンテンツはAmazon CloudFrontネットワークを通じて配信され、EU/EEA域外のエッジロケーションでトラフィックが処理される場合があります。
ClickHouse, Inc. (ClickHouse Cloud)	IPアドレスやブラウザ情報を含む、訪問数、参加数、登録数などのキャンペーン統計用の分析データベース	欧州連合（ドイツ、フランクフルト、AWS上にてホスト）。
Mailgun Technologies, Inc. (part of Sinch)	確認、コード、賞品通知など、データ管理者が設定した参加者へのメール送信（トラッキングが有効な場合の配信、開封、クリックを含む）	欧州連合（メッセージデータ用のEUリージョン）。限定的なアカウント情報がグローバルに処理される場合があります。
ip-api.com	不正行為やボットを防止するための、参加者のIPアドレスの大まかな位置情報の検索、及びプロキシやデータセンターからのトラフィックの検知	ルーマニア（EU）。EU/EEA域外での処理又はデータ移転の可能性を排除することはできません。
Google (Gemini API)	AIアシスタント、翻訳、テキスト生成など、本サービスにおけるAI機能。データ管理者のユーザーが直接入力しない限り、参加者データは仮名化又は集計された形式（イニシャル、メールのドメイン、登録日時など）でのみ送信されます	米国、及びAPIエンドポイントと処理設定によってはその他の国。

復処理者	処理の概要	処理の場所
Functional Software, Inc. (Sentry)	エラーの発見及び修復のための、本サービスのエラーモニタリング及びセッションリプレイ。レポートには、内部ユーザーID及びアカウントID、ならびにデータ管理者のユーザーのブラウザに関する技術データが含まれる場合があります。セッションリプレイ内のテキストはマスクされます	欧州連合（ドイツ、Sentry EUリージョン）。
Cloudflare, Inc. (Turnstile)	キャンペーンフォームでのボット保護（データ管理者がキャンペーンで有効にした場合のみ）。参加者のIPアドレスとブラウザシグナルを受信します	グローバルネットワーク。EU/EEA域外で処理が行われる場合があります。
Features & Labels, Inc. (fal.ai)	本サービスにおけるAI画像生成・編集、背景削除、ナレーション。データ管理者のユーザーが送信したプロンプトと画像を受信します	米国。
Adressevælger (adressevaelger.dk)	キャンペーンフォームでの住所自動入力候補の提示（データ管理者がキャンペーンで有効にした場合のみ）。参加者が入力した住所テキストと参加者のIPアドレスを受信します	デンマーク（EU）。

付録C – 技術的及び組織的措置

データ処理者は、Bureau VeritasによりISO/IEC 27001:2022の認証を受けた情報セキュリティマネジメントシステム（認証番号：FIHSK27150F）を維持しています。本措置には以下が含まれます。

- **ホスティング及び物理的セキュリティ：** すべてのカスタマーデータは、欧州連合内のAmazon Web Services（AWS）データセンターに保管されます。データ処理者は独自のサーバーを運用しておらず、物理的及び環境的セキュリティは、ISO 27001及びSOC 2の認証を受けているAWSによって提供されます。
- **ネットワークセキュリティ：**
  サーバー及びデータベースは、インターネットからアクセスできないプライベートネットワーク（Amazon VPC）内で動作します。ロードバランサーとコンテンツ配信ネットワークのみが公開されており、ウェブアプリケーシ

ョンファイアウォール（AWS WAF）とDDoS保護によって保護されています。

- **暗号化：** すべてのトラフィックはTLS (HTTPS)で暗号化されます。データベース、ファイル、バックアップは、AES-256で保管時に暗号化されます。連携用の資格情報は、アプリケーションレベルで追加で暗号化されます。パスワードは、bcryptによってハッシュ化及びソルト処理されます。
- **アクセス制御：**
  カスタマーユーザーに対する役割ベースのアクセス制御（RBAC）、2要素認証及びGoogleシングルサインオン、セッションタイムアウト、ログイン試行の回数制限。従業員のアクセス権は最小権限及び知る必要性（need-to-know）の原則に従い、固有のアカウントと可能な限りの多要素認証を使用し、少なくとも年に1回見直され、退職時には取り消されます。
- **データの分離：**
  カスタマーデータはアカウントごとに論理的に分離されており（テナントの隔離）、すべてのリクエストが認証・認可されます。
- **ログ記録及びモニタリング：**
  インフラストラクチャへの変更は改ざん防止機能付きの監査ログに記録され、アプリケーションログは一元的に収集され、プラットフォームは24時間体制で監視されます。カスタマーはアクティビティログで自社ユーザーのアクティビティを確認できます。
- **可用性及び障害復旧力：**
  少なくとも7日間保持され本番環境とは別に保管される毎日の暗号化バックアップ、少なくとも年に1回テストされるリストア作業、ならびに毎年見直され訓練される事業継続及び災害復旧計画。
- **インシデント管理：**
  第8条に基づくデータ侵害の通知を含む、セキュリティインシデントの報告、評価、封じ込め、分析及び事後対応を行う文書化されたプロセス。
- **安全な開発及び運用：**
  サーバーは手動で変更されることのないSSHアクセスなしのイミュータブル（不変）コンテナとして動作し、変更はリリース前にテストされます。
- **人的対策：**
  従業員は秘密保持義務を負い、情報セキュリティマネジメントシステムの一環として情報セキュリティ意識向上トレーニングを受けます。インフラストラクチャへのアクセス権を持つパートナーは、自社でISO 27001認証を取得しており、業務で必要なアクセス権のみが付与されます。
- **データの最小化及び消去ツール：**
  各キャンペーンで収集するデータはデータ管理者が決定し、参加者データのエクスポート、消去、又は自動消去を行う

ことができます。