# データ処理補足契約

| | |
|---|---|
| お客様: | |
| スプリンクラー: | **Sprinklr, Inc.**<br>29 W. 35th Street, New York, NY 10001, USA |

スプリンクラーは、お客様およびお客様の欧州関連企業にサービスを提供するにあたり、お客様およびお客様の欧州関連企業に代わって個人データを処理することができます。

データ処理補足契約（以下「DPA」といいます）は、お客様による下記の署名の日付から発効します。DPAは、お客様とスプリンクラーの間で締結されるスプリンクラーサービス契約（またはスプリンクラーのサービスの購入に関する他の契約）の一部を形成します。DPAを締結するお客様が、スプリンクラーサービス契約に従ってお客様とスプリンクラーの間で取り交わされるライセンス注文書（LOF）または作業指示書（SOW、またはスプリンクラーのサービスを購入する他の契約。以下、総称して「注文書」といいます）の当事者ではあるものの、スプリンクラーサービス契約の当事者ではない場合、DPAはそれぞれの注文書（更新がある場合は更新を含む）の一部を形成します。スプリンクラーサービス契約および／または注文書を総称して「本サービス契約」と呼ぶものとします。

DPAは、データ保護法の要件に従った個人データの処理に関する両当事者の合意を反映しています。

DPAは、お客様が本サービス契約（データ処理に関する本サービス契約の補足契約ですでに締結されたものを含む）において過去に交渉した個人データの処理に関する付加的な権利として置き換わるものではありません。

お客様はDPAに署名することにより、自らDPAの当事者となります。また、欧州関連企業に代わりその名前において締結する場合には、スプリンクラーと当該欧州関連企業の間でそれぞれ個別にDPAを締結します。それぞれの欧州関連企業は、DPAおよび適用される範囲内での本サービス契約に基づく義務を負うことに同意します。疑義を避けるために明記すると、欧州関連企業は本サービス契約の当事者ではなく、当事者となることもなく、DPAの当事者となるだけです。欧州関連企業がサービスにアクセスおよび利用する際は、必ず本サービス契約の契約条件に従って行われる必要があり、欧州関連企業が本サービス契約の契約条件に違反した場合はお客様が違反したものとみなします。契約当事者であるお客様は、DPAに基づきスプリンクラーとのすべての連絡を調整する責任を引き続き負うとともに、欧州関連企業の代理人としてDPAに関するすべての連絡を送付および受領する権限を持ちます。

**本DPAを構成する2つの部分:**

A. **データ処理に関する用語**
B. **標準契約条項**

| **お客様** |
| --- |
| |
| 署名者（氏名、役職）： |
| |
| 日付: |
| |
| 署名: |
| |

| **スプリンクラー** |
| --- |
| |
| 署名者（氏名、役職）： |
| Christian Schmoll, Director Legal EMEA & Privacy |
| 日付: |
| |
| 署名: |
| |

# A. データ処理に関する用語

## 1. 定義

**「関連企業」**とは、法主体を直接的または間接的に支配する主体、支配される主体、若しくは共同支配下にある主体を意味します。この定義において、「支配」とは、当該の法主体の議決権持ち分の 50%を超えて直接的または間接的に所有または管理することを意味します。

**「支配者」**とは、個人データの処理の目的および手段を決定する法主体を意味します。

**「データ保護法」**とは、本サービス契約に基づく個人データの処理に対して適用される、欧州連合、欧州経済領域およびその参加国、スイスおよび英国の法令を含むすべての法令を意味します。

**「データ主体」**の定義については、データ保護法に準じます。

**「欧州関連企業」**とは、（a）欧州連合、欧州経済領域およびその参加国、スイスおよび英国のデータ保護に関する法令の対象であり、（b）お客様とスプリンクラーの間の本サービス契約に従ってサービスの利用を許可されているが、自らはスプリンクラーへの注文書に署名していない、お客様の関連企業を意味します。

**「個人データ」**とは、（i）識別された、または識別可能な自然人に関する情報、（ii）識別された、または識別可能な法人に関連し、本サービス契約に基づくサービスの提供においてスプリンクラーがお客様の処理者として処理する情報（当該情報が個人情報または個人識別が可能な情報と同様に、データ保護法の下で保護されている場合）を意味します。

**「個人データの漏洩」**とは、送信され、保管され、又はその他の方法で処理される個人データが、セキュリティが侵害されたことにより、偶発的または違法に破壊され、喪失し、改変され、不正に開示され、またはアクセスされることを意味します。

**「処理」**の定義については、データ保護法に準じます。

**「処理者」**とは、管理者に代わって個人データを処理する者を意味します。

**「サービス」**とは、スプリンクラーが SaaS として提供する顧客体験およびソーシャルメディア管理プラットフォームおよび関連サービスを意味します。

**「復処理者」**とは、スプリンクラーまたはスプリンクラーの関連企業が業務に従事させる処理者を意味します。

**「ユーザー」**とは、本サービス契約に基づいてサービスを利用する資格を持つお客様、お客様の関連企業およびお客様の請負業者の従業員を意味します。

## 2. データ処理

**2.1** 両当事者は、個人データの処理に関して、お客様が管理者であり、スプリンクラーが処理者であることを承諾し、合意します。

**2.2** 両当事者は、データ保護法に準拠して、それぞれの義務を遵守するものとします。お客様はサービスの利用に際し、データ保護法の要件に従って個人データを処理するものとします。

**2.3** 個人データの処理に関するお客様の指示は、データ保護法を遵守したものでなければなりません。お客様からの指示がデータ保護法に違反すると考えられる場合、スプリンクラーはお客様に直ちに通知します。

**2.4** スプリンクラーは、(i) 本サービス契約に従った処理、(ii)サービスの利用に際してユーザーによって開始された処理、(iii) お客様が提供した他の合理的な指示書に従った処理を行うことを目的として、お客様の指示書に従って個人データを処理するものとします。

**2.5** スプリンクラーは個人データへのアクセスが可能な自社及び/または復処理者の従業員の信頼性を確保するための合理的な対策を実施するものとし、個人データへのアクセスを必要とする者を制限し、アクセスをする者が個人情報の取り扱いに関する法律の研修を受け、機密性の保持に努めることを確認するものとします。

**2.6** 処理の内容、期間、性質および目的、個人データの種類、データ主体のカテゴリーについては、付属の標準契約条項の付記事項1で定義します。

## 3. データ主体の権利の要請

**3.1** スプリンクラーがデータ主体から、データ主体のアクセス権、訂正権、処理の制限、消去（「忘れられる権利」）、データ携行性、異議申立、または自動的に個人の意思を決定されない権利を行使する要請（これらの要請を「DSR要請」といいます）を受けた場合、法的に許される範囲で速やかにお客様に通知するものとします。

**3.2** スプリンクラーは、お客様がデータ保護法の下でDSR要請に対応する義務を果たせるように、処理の性質を考慮して、適切な技術的および組織的対策により、可能な限りお客様を支援するものとします。

**3.3** お客様がサービスの利用に際してDSR要請に対応する能力を持たない場合に限り、スプリンクラーは、法的に許され、データ保護法に基づいてDSR要請への対応が必要な範囲において、お客様の要請を受け、お客様が当該のDSR要請に対応できるよう支援するために商業的に妥当な努力をするものとします。法的に許される範囲内で、お客様はスプリンクラーが当該支援を提供することによって生じる費用を負担するものとします。

## 4. データ保護の影響評価

スプリンクラーはデータ保護の影響評価に関して、スプリンクラーが個人データを処理する場合に限って、スプリンクラーが行うことのできる処理および使用可能な情報の性質を考慮して、合理的な支援と、データ保護法に基づいて必要とされる法的能力を有するデータ保護監督当局との事前協議をお客様に提供するものとします。

## 5. 個人データの漏洩の通知

**5.1** スプリンクラーは、個人データの漏洩を認識した後、遅滞なく、いかなる状況でも 48 時間以内にお客様に通知するものとします。スプリンクラーは、お客様が法的資格を有するデータ保護監督当局への通知義務を果たし、データ保護法に基づいて個人データの漏洩をデータ主体に連絡できるように、お客様に十分な情報を提供するものとします。

**5.2** スプリンクラーは、個人データの漏洩の原因を特定するために合理的な努力をし、スプリンクラーの合理的な管理の及ぶ範囲内において、当該個人データの漏洩の原因を解決するために必要かつ合理的と認める対策を実施するものとします。

**5.3** 本書において、お客様が引き起こした事故には義務を負わないものとします。

## 6. 復処理

**6.1** お客様は、スプリンクラーが標準契約条項の付記事項1の定義に従って復処理者を利用することに同意するものとします。

**6.2** スプリンクラーはそれぞれの復処理者と、復処理者が提供するサービスの性質に適用される範囲内で、個人データの保護という点でDPAの義務と同等の保護を行うデータ保護義務を含む契約を書面によって交わしています。

**6.3** スプリンクラーがDPAの条件の下でそれぞれの復処理者のサービスを直接提供する場合、本サービス契約に別途規定のない限り、スプリンクラーは復処理者の行為および不作為について法的責任を負います。

## 7. セキュリティ

スプリンクラーは添付された標準契約条項の付記事項2の規定に従って、適切な技術的および組織的セキュリティ保護（個人データの不正または違法な処理からの保護、並びに偶発的または違法な破壊、喪失、改変、不正開示またはアクセスからの保護を含む）の対策、個人データの機密性および完全性を維持するものとします。スプリンクラーはこれらの対策の遵守を定期的に監視します。スプリンクラーは本サービス契約の期間中、サービス全体のセキュリティ性を実質的に低下させません。

## 8. 個人データの削除または返却

**8.1** スプリンクラーは、本サービス契約の規定に従って本サービス契約の終了または満了と同時に、またはお客様からの合理的な要請を受けて随時、個人データを削除するものとします。スプリンクラーは適用法によって必要とされる範囲内で、適用法によって必要とされる範囲および期間においてのみ、すべての当該個人データの機密性を確保すること、および当該個人データが他の目的のためではなく適用法に定められている目的のため保管が必要であ

る場合のみ処理されることを条件として、個人データを保持することができます。

**8.2** スプリンクラーは、本サービス契約に規定されている手順および期間に従って、個人データをお客様に返却するものとします。

## 9. 監査および視察

**9.1** スプリンクラーは、DPAの遵守を証明するために必要なすべての情報をお客様に提供し、個人データの処理に関してお客様による監査を受け入れ、協力するものとします。スプリンクラーは、お客様の書面による要請を受け、１年に1回まで、お客様から提供されたスプリンクラーのデータ保護および情報セキュリティに関するプラクティスおよびポリシーについての合理的な情報セキュリティ質問票に対して正確に回答します。

**9.2** お客様、またはお客様から委任された第三者監査人は、10営業日前までに書面による事前通知を合理的に行うことにより、お客様の負担で1年に1回まで、スプリンクラーのデータ保護および情報セキュリティに関するプラクティスおよびポリシーの現場視察を行うことができます。視察は1日を限度とし、監査がスプリンクラーの業務運営に及ぼす影響を最小限に留めるように双方が同意したスケジュールで通常の営業時間内に行うものとします。お客様、またはお客様から委任された第三者監査人は、視察の実行について、スプリンクラーのセキュリティ要件を遵守するものとします。機密性およびセキュリティ要件のため、当該視察ではマルチテナント環境（スプリンクラーが使用するIaaSデータセンターなど）の現場視察は除外されます。当該環境の現場調査は、実施されているそれぞれのデータ保護およびセキュリティ対策に関する詳細文書および信頼できる第三者監査人が発行する特定の証明書をお客様の要請に応じてスプリンクラーが提供することによって代替できます。

**9.3** お客様は当該の監査または視察の実施中に発見した不遵守について、スプリンクラーに速やかに通知するものとします。

## 10. 法的責任

**10.1** DPAおよび欧州関連企業とスプリンクラーの間のすべてのDPAに起因または関連する各当事者の法的責任は、契約から生じるものであるか、不法行為であるか、又はその他の法的根拠に基づく責任であるかどうかにかかわらず、本サービス契約に基づいて合意した法的責任制限の項が適用され、当該項に規定されている当事者の法的責任とは、本サービス契約およびすべてのDPAに基づいて当該の当事者および関連企業が負う累積的責任を指します。

**10.2** 疑義を避けるために明記すると、DPAおよび各DPAに起因または関連するお客様およびそのすべての欧州関連企業からのすべての請求に対するスプリンクラーの累積的責任は、お客様およびすべての欧州関連企業によるものを含め、本契約に基づいて締結された本サービス契約およびすべてのDPAの両方に基づくすべての請求全体に適用されるものとし、特に、当該DPAの契約当事者であるお客様または欧州関連企業に対して個々別々に適用されるものと解釈されてはなりません。

**10.3** また、疑義を避けるために明記すると、DPAにおいては、DPAとは標準契約条項を含むDPAを指します。

**10.4** データ主体がGDPR第82条に従ってDPAの一方の当事者に対して損害賠償を請求する場合、他方の当事者は可能な限り、当該請求に対する防御を支援するものとします。

## 11. 標準契約条項

**11.1** 添付されている標準契約条項は、DPAに基づいて、欧州連合、欧州経済領域およびその参加国、スイスおよび英国から、前述の地域のデータ保護法の意義の範囲内で十分なレベルのデータ保護を確保していない国に対して個人データの移転が行われる場合には、当該移転がデータ保護法の支配下にある限りにおいて適用されるものとします。

**11.2** データ処理に関するこれらの用語と標準契約条項の間で矛盾または不一致がある場合は、標準契約条項を優先するものとします。

## B. 標準契約条項

**十分なレベルの保護を確保していない第三国で設立された処理者への個人データの移転に関する、第 26 条(2)項の指令 95/46/EC の解釈に関する欧州委員会決定 C(2010)593**

| **データ輸出組織** | |
|---|---|
| 名称: | |
| 所在地: | |
| 電話/Fax/メール: | |
| お客様はお客様のために、またはその欧州関連企業に代わりその名前において、これらの標準契約条項に同意します。 | |
| 以下「データ輸出者」といいます。 | |

| **データ輸入組織** | |
|---|---|
| 名称: | Sprinklr, Inc. |
| 所在地: | 29 West 35th Street, New York, NY 10001, USA |
| 電話/Fax/メール: | +1-917-933-7800; fax: n/a; e-mail: privacy@sprinklr.com |
| 以下「データ輸入者」といいます。 | |

各々を「各当事者」、両者を合わせて「両当事者」といいます。

上記の者は、データ輸出者からデータ輸入者に対する個人データ（付記事項 1 に記載されているもの）の移転における、個人のプライバシー、基本的権利および自由の保護に関する十分な保護措置を提示するため、以下の契約条項（以下「本契約条項」という）に合意しました。

### 第 1 条: 定義

本契約条項において、以下の用語は、以下の意味を有するものとします。

(a)「個人データ」、「特別カテゴリーのデータ」、「処理」、「管理者」、「処理者」、「データ主体」および「監督当局」は、個人データの処理に係る個人の保護および当該データの自由な移動に関する 1995 年 10 月 24 日の欧州議会および理事会の指令 95/46/EC における定義と同じ意味を有します。

(b)「データ輸出者」とは、個人データを移転する管理者を意味します。

(c)「データ輸入者」とは、データ輸出者の指示および本契約条項の条件に従い、移転した後にデータ輸出者に代わって処理を行うことが予定されている個人データを、データ輸出者から受領することに同意する処理者であり、指令 95/46/EC の第 25 条(1)項での意味における十分な保護を確保する第三国の制度に服していない者を意味します。

(d)「復処理者」とは、データ輸入者またはデータ輸入者の他の復処理者から業務を請け負う者であって、データ輸入者またはデータ輸入者の他の復処理者から個人データ（データ移転後に、データ輸出者の指示、本契約条項の条件および書面による下請契約の条件に従い、データ輸出者に代わって処理を行うことのみを目的とした個人データ）を受領することに同意した者を意味します。

(e)「適用されるデータ保護法令」とは、データ輸出者が設立された EU 加盟国においてデータ管理者に適用される、個人の基本的権利および自由（特に、個人データの処理に関するプライバシー権）を保護する法律を意味します。

(f)「技術的および組織的セキュリティ対策」とは、特にネットワークを通じた送信による処理が行われる場合の偶発的または違法な破壊、偶発的な喪失、改変、不正開示またはアクセス、およびその他のあらゆる違法な処理形態から個人データを保護することを目的とする対策を意味します。

## 第 2 条: 移転の詳細

移転（該当する場合は、特に特別カテゴリーの個人データ）の詳細は、本契約条項の不可分な一部を構成する付記事項 1 に記載します。

## 第 3 条: 第三者受益者条項

1. データ主体は、第三受益者として、データ輸出者に対し、本条、第 4 条(b)項から(i)項まで、第 5 条(a)項から(e)項まで、および(g)項から(j)項まで、第 6 条(1)項および(2)項、第 7 条、第 8 条(2)項、並びに第 9 条から第 12 条までの権利を行使することができます。

2. データ主体は、データ輸出者が事実上消滅した、または法律上存在しなくなった場合、データ輸入者に対し、本条、第 5 条(a)項から(e)項まで、(g)項、第 6 条、第 7 条、第 8 条(2)項、並びに第 9 条から第 12 条までの権利を行使することができます。ただし、データ輸出者の承継人が、契約または法律により、データ輸出者の法的義務をすべて引き受け、その結果、当該承継人がデータ輸出者の権利義務を承継した場合を除きます。その場合、データ主体は、当該承継人に対してこれらの権利を行使することができます。

3. データ主体は、データ輸出者およびデータ輸入者の双方が事実上消滅した、若しくは法律上存在しなくなった場合、またはこれらの双方が支払不能に陥った場合、復処理者に対し、本条、第 5 条(a)項から(e)項までおよび(g)項、第 6 条、第 7 条、第 8 条(2)項、並びに第 9 条から第 12 条までの権利を行使することができます。ただし、データ輸出者の承継人が、契約または法律により、データ輸出者の法的義務をすべて引き受け、その結果、当該承継人がデータ輸出者の権利義務を承継した場合を除きます。その場合、データ主体は、当該承継人に対してこれらの権利を行使することができます。データ復処理者の第三者の法的責任は、本契約条項に基づく自身の処理業務に限定されるものとします。

4. 両当事者は、データ主体が希望し、かつ国内法上許容されている場合、協会またはその他の機関がデータ主体を代理することに異議を申し立てません。

## 第 4 条: データ輸出者の義務

データ輸出者は、以下に同意し、以下を保証します。

(a) 個人データの処理（個人データの移転自体を含む）が、適用されるデータ保護法令に従い実施されてきた、また今後も引き続き上記法令に従って実施されること、（また、該当する場合は、データ輸出者が設立された EU 加盟国の関係当局に通知を行っていること）、さらに当該加盟国の関連条項に違反しないこと。

(b) データ輸入者に対し、適用されるデータ保護法令および本契約条項に従って、移転された個人データの処理を当該データ輸出者のためにのみ行うよう指示してきたこと、また、個人データ処理サービスの継続期間を通じて同指示を行うこと。

(c) データ輸入者は、本契約の付記事項 2 に記載されている技術的および組織的セキュリティ対策に関して、十分な保証を与えること。

(d) 適用されるデータ保護法令の要件の評価後、セキュリティ対策が、特にネットワークを通じた送信による処理が行われる場合に偶発的または違法な破壊、偶発的な喪失、改編、不正開示またはアクセス、およびその他のあらゆる違法な処理形態から個人データを保護するために適切なものであること、また、これらの対策が、最新の技術と対策実施費用を考慮した上で、処理およびデータの性質により生じるリスクを回避できるよう適切なレベルのセキュリティを確保するものであること。

(e) セキュリティ対策の確実な遵守を図ること。

(f) 当該移転に特別カテゴリーのデータが含まれる場合、データ主体に対し、当該データ主体のデータが指令 95/46/EC の意義の範囲で十分な保護が提供されていない第三国に移転される可能性がある旨を通知済みであること、若しくは事前に通知すること、または事後に可能な限り速やかに通知すること。

(g) 第 5 条(b)項および第 8 条(3)項に基づきデータ輸入者または復処理者から受領した通知を、データ保護監督当局に転送すること。ただし、データ輸出者が、移転の継続または移転の一時停止を解除する旨を決定した場合に限ります。

(h) 要請に応じ、データ主体に対し、本契約条項のコピー1 部（ただし、付記事項 2 は例外とします）およびセキュリティ対策の概要、並びに復処理サービスに関する契約書（この契約は本契約条項に従って作成されなければなりません）のコピー1 部を提供すること。ただし、本契約条項または復処理サービス契約に商業上の情報が含まれる場合、データ輸出者は、当該商業上の情報を除外することができます。

(i) 復処理が行われる場合、データ主体の個人データおよび権利に対し、少なくとも本契約条項におけるデータ輸入者と同レベルの保護を提供する復処理者によって第 11 条に従って当該処理業務が実施されること。

(j) 第 4 条(a)項から(i)項までの遵守を確保すること。

## 第 5 条: データ輸入者の義務

データ輸入者は、以下に同意し、以下を保証します

(a) 個人データの処理を、データ輸出者の指示および本契約条項に従って、データ輸出者のためにのみ行うこと。何らかの理由により上記を遵守することができない場合、データ輸入者は、速やかにその旨をデータ輸出者に通知することに同意します。この場合、データ輸出者は、データ移転を一時停止する権利または本契約を解除する権利を有します。

(b) データ輸入者に適用される法令により、データ輸出者からの指示の遂行および本契約に基づく自身の義務の履行が妨げられると信じる理由がないこと。また、本契約条項に規定された保証および義務に実質的に悪影響を及ぼすおそれのある上記法令の改正が行われた場合、データ輸入者は、当該変更を認識した後速やかにデータ輸出者に対して当該変更を通知すること。この場合、当該データ輸出者は、データ移転を一時停止する権利または本契約を解除する権利を有します。

(c) 移転された個人データの処理を行う前に、付記事項 2 に記載されている技術的および組織的セキュリティ対策を実施していること。

(d) 以下のいずれかの事情が生じた場合には、データ輸出者に速やかに通知すること。

(i) 法執行機関から、法的拘束力を有する個人データの開示要請を受けた場合。ただし、通知を行うことが禁止されている場合（例えば、法執行機関の捜査の秘密性を維持するため刑事法により禁止されている場合）を除きます。

(ii) 偶発的または不正アクセス。

(iii) データ主体から直接受けた要請。別途許可されている場合を除き、要請には対応しません。

(e) 移転の対象である個人データの処理に関するデータ輸出者からのすべての質問を、迅速かつ適切に処理すること。また、移転されたデータの処理に関する監督当局からの助言に従うこと。

(f) データ輸出者の要請に応じ、データ輸出者または検査機関（監督当局との合意により（該当する場合）、データ輸出者により選定された、独立性および必要とされる専門的資格を有し、秘密保持義務を負うメンバーにより構成される）が実施する、本契約条項の対象となる処理活動の監査のためにデータ処理設備を提供すること。

(g) 要請に応じ、データ主体に対し、本契約条項またはデータの復処理に関する既存の契約書のコピー1 部を提供すること（ただし、本契約条項または上記復処理契約に商業上の情報が含まれる場合は、当該商業上の情報を非開示とすることができます）。ただし、付記事項 2 については、データ主体がそのコピーをデータ輸出者から入手できない場合は、セキュリティ対策の概要で代替するものとします。

(h) データの復処理が行われる場合、事前にデータ輸出者に通知し、事前の書面による同意を取得していること。

(i) 復処理者による処理サービスが、本契約条項の第 11 条に従って実施されること。

(j) 本契約条項に基づき締結されたデータの復処理契約書のコピー1 部を、速やかにデータ輸出者に送付すること。

## 第 6 条: 法的責任

1. 両当事者は、当事者のいずれかまたは復処理者が本契約条項の第 3 条または第 11 条に違反したことによって損害を被ったデータ主体が、当該損害について、データ輸出者から賠償を受ける権利を有することに同意します。

2. データ輸出者が事実上消滅したか、法律上存在しなくなったか、または支払不能に陥ったことにより、データ主体がデータ輸出者に対し、データ輸入者または復処理者が第 3 条または第 11 条に基づく義務に違反したことに起因する第 1 項に基づく賠償請求をすることができない場合、データ輸入者は、データ主体がデータ輸入者をデータ輸出者と同視し、データ輸入者に対して請求を行うことができることに同意します。ただし、データ輸出者の承継人が、契約または法律により、データ輸出者の法的義務をすべて引き受けた場合を除くものとし、その場合、当該データ主体は、当該承継人に対して権利を行使することができます。データ輸入者は、復処理者による違反であることを理由として自身の法的責任を回避することはできません。

3. データ輸出者およびデータ輸入者の双方が事実上消滅したか、法律上存在しなくなったか、またはこれらの双方が支払不能に陥ったために、データ主体が第 1 項および第 2 項に定めるデータ輸出者またはデータ輸入者に対する請求を、復処理者が第 3 条または第 11 条に規定された義務に違反したことに起因する請求を行うことができない場合、復処理者は、本契約条項に基づく処理業務に関して、復処理者をデータ輸出者またはデータ輸入者と同視して、データ主体が復処理者に対して請求を行うことができることに同意します。ただし、データ輸出者またはデータ輸入者の承継人が、契約または法律により、データ輸出者またはデータ輸入者の法的義務をすべて引き受けた場合を除きます。その場合、データ主体は、当該承継人に対して自身の権利を行使することができます。復処理者の法的責任は、本契約条項に基づく自身の処理業務に限定されるものとします。

## 第 7 条: 仲介および裁判管轄

1. データ輸入者は、データ主体が本契約条項に基づきデータ輸入者に対して第三受益者としての権利を行使した、または損害賠償請求を行った場合、データ主体による以下の決定に従うことに同意します。

   (a) 当該紛争を、独立した個人、または監督当局（該当する場合）による調停に付託すること。

   (b) 当該紛争を、データ輸出者が設立された EU 加盟国の裁判所に付託すること。

2. 両当事者は、データ主体による選択が、データ主体が国内法または国際法の他の条項に従って救済を求める実体的権利または手続的権利に影響を与えないことに同意します。

## 第 8 条: 監督当局との協力

1. データ輸出者は、監督当局から要請された場合、または適用されるデータ保護法令に基づいて必要とされる場合、本契約書のコピー（1 部）を監督当局に預けることに同意します。

2. 両当事者は、監督当局がデータ輸入者および復処理者の監査（適用されるデータ保護法令に基づくデータ輸出者に対する監査と同じ範囲であり、前記監査に適用される条件と同一の条件に従う）を行う権利を有することに同意します。

3. データ輸入者は、データ輸出者に対し、第 2 項に基づくデータ輸入者または復処理者の監査の実施を妨げる、データ輸入者または復処理者に適用される法規が存在する場合に、データ輸出者に速やかに通知するものとします。この場合、データ輸出者は、第 5 条(b)項で想定される措置を実施する権利を有します。

## 第 9 条: 準拠法

本契約条項は、データ輸出者が設立された EU 加盟国の法律に準拠するものとします。

## 第 10 条: 契約の変更

両当事者は、本契約条項の変更または修正を行わないことを約束します。ただし、両当事者が、本契約条項と矛盾しない範囲で、必要に応じて商取引上の条項を追加することは妨げられません。

### 第 11 条: 復処理

1. データ輸入者は、データ輸出者の事前の書面による同意がある場合を除き、データ輸入者が本契約条項に基づいてデータ輸出者のために履行する処理業務を第三者に委託してはなりません。データ輸入者が、データ輸出者の同意を得て本契約条項に基づく自身の義務を第三者に委託する場合、データ輸入者は、本契約条件に基づきデータ輸入者に課されるものと同一の義務を復処理者に課す契約を書面で締結することによってのみ、当該の復処理の委託を行うものとします。復処理者が当該の書面による契約に基づくデータ保護義務の履行を怠った場合、データ輸入者は、データ輸出者に対し、当該契約に基づく復処理者の義務の履行を完遂する責任を負います。

2. データ輸出者またはデータ輸入者が事実上消滅した、若しくは法律上存在しなくなった、またはこれらの双方が支払不能に陥った場合、かつ契約または法律によりデータ輸出者またはデータ輸入者の法的義務をすべて引き受ける承継人が存在しないため、データ主体が第 6 条 1 項に規定された損害賠償の請求をデータ輸出者またはデータ輸入者に対して行うことができない場合に備え、データ輸入者と復処理者との間の事前の書面による契約には、第 3 条に定められている第三受益者条項を規定するものとします。データ復処理者の第三者に対する法的責任は、本契約条項に基づく自身の処理業務に限定されるものとします。

3. 第 1 項に定める、契約に基づく復処理におけるデータ保護の観点に関する規定は、データ輸出者が設立された EU 加盟国の法律に準拠するものとします。

4. データ輸出者は、本契約条件に基づいて締結され、第 5 条(j)項に従ってデータ輸入者から通知された復処理契約のリストを保管するものとします。当該リストの更新は、少なくとも 1 年に 1 回行われるものとします。当該リストは、データ輸出者のデータ保護監督当局も入手することできるものとします。

### 第 12 条: 個人データ処理サービスの終了後の義務

1. 両当事者は、データ処理サービスの提供の終了時に、データ輸入者および復処理者が、データ輸出者の選択に従い、移転されたすべての個人データおよびそのコピーをデータ輸出者に返却するか、またはすべての個人データを破棄し、データ輸出者に対して破棄を行った旨を証明することに同意します。ただし、データ輸入者に適用される法律により、データ輸入者が移転されたデータの全部または一部の返還または破棄することができない場合を除きます。その場合、データ輸入者は、移転された当該個人データの秘密を保証することおよび当該個人データのデータ処理を積極的に行わないことを保証します。

2. データ輸入者および復処理者は、データ輸出者または監督当局の要請に応じ、第 1 項に規定された措置の監査のため、データ処理設備を提供することに同意します。

## 標準契約条項の付記事項

**データ輸出者**

データ輸出者は、スプリンクラーのカスタマー エクスペリエンスおよびソーシャル メディア マネジメント プラットフォームの使用許諾を受けたユーザーです。

**データ輸入者**

データ輸入者は、スプリンクラープラットフォーム（SaaS）を提供します。

**データ主体**

移転される個人データは、以下のカテゴリーのデータ主体に関するものです。

1. データ主体には、スプリンクラープラットフォームを運用して、データ輸出者のお客様、フォロワー、ファン、その他のソーシャルネットワークおよびウェブサイトを使用するインターネットユーザー、データ輸出者の従業員、データ輸出者の代理人、データ輸出者の下請業者の従業員と連携し協業する個人を含みます（「アカウント情報」）。

2. 移転される個人データは、データ輸出者がスプリンクラープラットフォームにアップロードまたはインポートする、データ輸出者のお客様、見込み客、その他のソーシャルネットワークおよびウェブサイトを使用するインターネットユーザーにも関連します（「カスタマーコンテンツ」）。
3. 移転される個人データは、データ輸出者のお客様、フォロワー、ファン、その他のソーシャルネットワークおよびウェブサイトを使用するインターネットユーザーにも関連する。当該ソーシャルネットワークおよびウェブサイトには現在、Twitter、Facebook、YouTube、LinkedIn、Google+、SlideShare、Instagram、Vkontakte、Sina Weibo、RenRen、WeChat、QQ ブログおよびブログのコメント、メインストリーム ニュース ソースおよびフォーラム、またデータ輸出者が所有し、データ輸入者がデータ輸出者に代わってソーシャルおよびコンテンツ管理機能を提供するウェブサイトが含まれるが、これに限定されません（「ソーシャルデータ」）。

**データのカテゴリー**

移転される個人データは、以下のカテゴリーのデータに関するものです。

1. 移転されるアカウント情報は、識別データ（名前、ログイン名）、連絡先情報（仕事用電子メールアドレス）、業務関連データ（利用またはパフォーマンスデータ、ソーシャル連絡先取り扱いデータ）に関するものです。
2. 移転されるカスタマーコンテンツは、データ輸出者がスプリンクラープラットフォームにアップロードまたは保管する個人データのカテゴリーに関するものです。
3. 移転されるソーシャルデータは、ソーシャルメディアユーザーがお客様のソーシャルメディアプロファイル（例：お客様の Facebook ページ）を通じて投稿または送信され、スプリンクラープラットフォーム（お客様に対する公開と非公開の両方のメッセージ）に接続され、お客様が定義した特定の検索クエリー（例：#customer）に基づいてソーシャルメディアネットワークおよびウェブサイトからのパブリックアクセスが可能なデータコンテンツに関するものです。ソーシャルデータには、ユーザーID または広告 ID、ソーシャルネットワークのプロファイル名および情報、ソーシャルネットワークの通信、ソーシャルメディアネットワークおよびウェブサイトで共有されたすべての種類の情報が含まれます。

**特別カテゴリーのデータ（該当する場合）**

移転される個人データは、以下の特別カテゴリーのデータに関するものです。

1. 移転されるカスタマーコンテンツには、データ輸出者がスプリンクラープラットフォームにアップロードまたは保管するデータの種類によっては、特別カテゴリーのデータが含まれることがあります。
2. 移転されるソーシャルデータには、データ輸出者がスプリンクラープラットフォームを使用する方法（例：ソーシャルメディアネットワークでのパブリックアクセスが可能な個人データを収集するための特定の検索クエリーの定義）によっては、特別カテゴリーの個人データが含まれることがあります。

**処理業務**

移転される個人データは、以下の基本的な処理活動の対象となります（明記してください）。

1. 移転されるアカウント情報は、スプリンクラープラットフォームの運用（認証、ログイン、監査証跡）のみを目的として処理されます。
2. 移転されるカスタマーコンテンツおよびソーシャルデータは、ソーシャルメディア管理を目的として処理されます。これには、ソーシャル メディア リスニングおよびアナリティクス、カスタマーケアおよびサポート、マーケティングアナリティクスおよびマーケティング管理が含まれます。

**指示**

DPA および本サービス契約は、個人データの処理のためスプリンクラーへの DPA に署名された時点で、輸出者の完全な指示になります。その他の追加または代替の指示については、別途合意しなければなりません。標準契約条項の条項 5(a) 項の解釈上、以下をお客様による個人データの処理指示とみなします。(i) 本サービス契約に従った処理。(ii) サービスの利用に際してユーザーによって開始された処理。(iii) お客様が提供する他の合理的な指示書に従った処理。

**復処理**

データ輸入者（スプリンクラー）がDPAの発行日付で契約サービスを提供するために利用する復処理者は、その役割および復処理の範囲、復処理の地理的範囲を含め、スプリンクラーの復処理者リスト（www.sprinklr.com/legal でアクセス可能）で公開されます。

当該復処理者は、標準契約条項第5条(h)および第11条に従ってデータ輸出者（お客様）の合意および同意を得るものとします。

データ輸入者（スプリンクラー）は、以下のとおり、他の適切かつ信頼できる復処理者を解任または選任することができます。

- データ輸入者（スプリンクラー）は、少なくとも30日前に、電子的手段によって、データ輸出者（お客様）の個人データへのアクセス権を復処理者に付与することで（ただし、以下に定める緊急時の交替を除く）、データ輸出者（お客様）に対し復処理者のリストの変更を通知することができます。
- データ輸出者（お客様）にデータ輸入者（スプリンクラー）が復処理者を使用することに異議を唱える正当かつ重大な理由がある場合、データ輸出者（お客様）はデータ輸出者（スプリンクラー）にデータ輸入者（スプリンクラー）の通知を受領してから15日以内にその旨を書面で通知するものとします。
- データ輸出者（お客様）が当該期間に異議を唱えない場合、新しい復処理者は標準契約条項第5条(h)および第11条に従ってデータ輸出者（お客様）の書面による合意および同意を得るものとします。
- データ輸出者（お客様）が当該復処理者の使用に異議を唱える場合、データ輸入者（スプリンクラー）は、以下の選択肢のいずれかを通じて異議を解決する権利を有します。(i) データ輸入者（スプリンクラー）は、データ輸出者（お客様）の顧客データに関して、復処理者の使用計画を中止します。(ii) データ輸入者（スプリンクラー）は、データ輸出者（お客様）が異議において要請する（データ輸出者（お客様）の異議を解決する）是正措置を講じ、データ輸出者（お客様）の個人データに関して復処理者を使用します。(iii) データ輸出者（お客様）の個人データに関する復処理者の使用を伴うサービスの特定の面において、データ輸入者（スプリンクラー）がその提供を停止するか、データ輸出者（お客様）がその不使用に（一時的または恒久的に）同意することができます。
- 前記の選択肢のいずれも合理的に使用できず、データ輸入者（スプリンクラー）がデータ輸出者（お客様）の異議を受領してから15日以内に異議が解決されない場合、各当事者は事前の書面による合理的な通知により、影響を受けるサービスを解約することができます。

「緊急時の交替」とは、（復処理者が廃業する、データ輸入者（スプリンクラー）へのサービスを突如終了する、データ輸入者（スプリンクラー）に対する契約上の義務に違反するなど）、データ輸入者（スプリンクラーの）の合理的な支配の及ばない範囲で変更が生じた場合に復処理者が実施する急な交替を指します。その場合、データ輸入者（スプリンクラー）はできるだけ速やかに、データ輸出者（お客様）に対し、承継する復処理者を通知し、前記の当該復処理者を正式に指名するプロセスを開始するものとします。

標準契約条項の第5条(j)項に従って提供されなければならない復処理者契約のコピーでは、すべての商業情報、若しくは標準契約条項に関連のない条項またはこれに相当する内容を、スプリンクラーが事前に削除することができます。また、スプリンクラーは、お客様からの要請を受けた場合のみ、当該コピーを任意の方法で提供します。

**監査および視察**

標準契約条項の第5条(f)項および第12条(2)項は、DPAの9節に従って実施されるものとします。

**削除の証明**

スプリンクラーは、お客様からの要請を受けた場合のみ、標準契約条項の第12条(1)項に規定されている個人データの削除の証明をお客様に提供します。

# 標準契約条項の付記事項 2

**第 4 条(d)項および第 5 条(c)項に従い、データ輸入者が講じた技術的および 組織的セキュリティ対策の説明（または文書若しくは法律を添付）：**

**1. データ保管およびネットワークセキュリティ**

**(a) データ保管**

インフラストラクチャ。データ輸入者は、データ保管のため、Amazon Web Service (AWS)または Microsoft Azure を使用します。データ輸入者は、これらの安全なサービスを通じて、すべての本番データを保管します。ウェブサービスセキュリティプロセスの概要は以下のとおりです。

- http://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf and
- https://azure.microsoft.com/en-us/services/security-center/

**(b) ネットワークセキュリティ**

災害復旧目標。大規模災害が発生した場合、24 時間以内にサービスを完全に復旧するために、すべてのプロセスおよび従業員を配置します。RTO（目標復旧時間）は 24 時間、RPO（目標復旧時点）は 24 時間です。

高可用性。スプリンクラーアプリケーションは 25 を超える独立サービスで構成されます。1 つのサービスコンポーネントにつき、少なくとも 2 つのインスタンスが米国の 2 つの異なるゾーン（データセンター）で常に実行されます。ゾーンはそれぞれ異なる場所にあり、他方のゾーンでの障害から隔離されるように設計されます。

災害復旧。セカンダリサイトでバックアップデータおよびコードからサービスを復旧するための自動化プロセスが設置されます。自動化により、定められた RPO および RTO の目標内で十分にサービス全体が復旧されます。

冗長性。インフラストラクチャシステムは、単一障害点を排除し、予期しない環境リスクの影響を最小限に留めるように設計されます。サービスは、データ輸入者がサービスを中断することなく、特定の種類の予防措置および是正措置を講じることができるように設計されます。

サーバーのオペレーティングシステム。データ輸入者のサーバーでは、アプリケーション環境に合わせてカスタマイズした Linux ベースのオペレーティングシステムを使用します。データ輸入者は、サービスを提供するために使用されるコードのセキュリティを向上し、本番環境のセキュリティを強化するために、コードレビュープロセスを導入します。

事業継続性。データ輸入者は、データの意図しない破壊または喪失の可能性を抑制するために、データを複数のシステムに複製します。データ輸入者は事業継続計画または災害復旧プログラムを設計し、定期的にテストします。

**(c) ネットワークおよび伝送**

インシデント対応。データ輸入者はセキュリティインシデントに備えてさまざまな通信チャネルを監視し、データ輸入者のセキュリティ関係者は検知されたインシデントに速やかに対応します。

暗号化技術。データ輸入者はすべての接続に HTTPS 暗号化（SSL または TLS ともいう）を要請します。ウェブセッションは HTTPS を使用して暗号化され、スプリンクラーアプリケーションとの安全なデータ通信が提供されます。バックエンドサーバーへのアクセス（サポート用）は、SSH、SFTP および RDP で行います。

**2. アクセスおよびサイト制御**

制御アクティビティおよびプロセス。制御アクティビティにより、関連アプリケーション、データおよびシステムリソースへの論理アクセスが適切に許可された個人およびプログラムに制限されていることの合理的な保証を提供します。スプリンクラーの技術運用チームは、ファイアウォールおよびセキュリティグループの設定および管理を担当し、スプリンクラープラットフォームのセキュリティおよびアクセスを制御します。

バックエンドインフラストラクチャには 2 つのレベルのアクセスメカニズムを必要とします。Linux サーバーでは、公開鍵ベースの SSH 認証を使用してアクセスサーバーにアクセスします。アクセスサーバーからは、LDAP 認証を使用して他のサーバーにアクセスします。LDAP 認証はユーザーID およびパスワードに基づきます。Windows サーバーでは、両側で RDP over SSL を使用します。

アプリケーションへのアクセスは HTTPS を介して行われ、安全な暗号化されたトランスポートセッションでアプリケーションに接続されます。スプリンクラーは、役割（ロール）ベースのアクセス制御（RBAC）アプローチでユーザーアクセスを提供します。このアプローチでは、役割に基づいて必要な機能のみへのユーザーアクセスが決定されます。

システムによって使用されるすべての機密データは暗号化された状態で保管され、データストアインスタンスへの直接アクセス権はデータベース管理者のみに付与されます。エンドユーザーはデータストアに直接アクセスできません。エンドユーザーのアクセスはアプリケーションを介してのみ可能です。

SOC 1 Type I および II、並びに SOC 2 Type I および II の調査の完了は、お客様に提供するサービスにおいて最高品質およびセキュリティを確保するために必要な最も厳しい管理策の作成および維持にスプリンクラーが継続的に取り組んでいることを表します。

システムは Amazon Elastic Compute Cloud (EC2) マネージドサービスを通じて Linux および Windows サーバーインスタンスで展開され、それによって OS レベルのパッチを含む信頼性と柔軟性を備えたサーバーデプロイメントを可能にします。

ファイアウォールおよびホストベースの侵入検知システムがシステムに導入されています。すべてのセキュリティ監視システム（ファイアウォール、ホスト侵入検知システムを含むが、これに限定されない）が導入され、有効化されます。

すべてのインフラストラクチャプラットフォームおよびサービス（オペレーティングシステム、ウェブサーバー、データベースサーバー、ファイアウォールなど）が業界のベストプラクティスに従って設定されます。スプリンクラーの IT オペレーションチームは、セキュリティグループを使用したファイアウォールの設定および管理を担当し、「内部」ネットワークインフラストラクチャのセキュリティおよびアクセスを制御します。

データ輸入者は、従業員向けセキュリティポリシーを策定および維持し、従業員向け研修パッケージの一部としてセキュリティ研修を義務付けます。データ輸入者のインフラストラクチャのセキュリティ担当者は、データ輸入者のセキュリティインフラストラクチャの継続的な監視、サービスの検証、セキュリティインシデントへの対応を行います。

アクセスおよび権限管理。データ輸出者の管理者およびエンドユーザーは、サービスを使用するために、集中認証システムまたはシングルサインオンシステムを通じて認証を行わなければなりません。各アプリケーションでは、許可されたユーザーまたは許可された管理者にデータを表示するために、資格情報をチェックします。

**3. データ**

データ保管、隔離、認証、バックアップおよび復旧。本番環境データベースの完全なスナップショットを毎日作成します。スプリンクラーのクラウドベンダーによって提供されたツールを使用してデータベースバックアップ（DB）を作成し、オンデマンドで（重要リリースの際に）データベーススナップショット（DB スナップショット）を作成します。自動バックアップにより、DB インスタンスのポイントインタイムリカバリを可能にします。スプリンクラーはデータの完全な日次スナップショットを作成し、（DB インスタンスの更新が行われた場合は）トランザクションログを取得します。ポイントインタイムリカバリを開始した場合、DB インスタンスを必要とされる特定の時点に復旧させるために、トランザクションログを最新の適切な日次バックアップに適用します。

**4. 従業員に関するセキュリティ**

データ輸入者の従業員は、機密性、ビジネス倫理、適切な使用、職業上の基準に関する自社のガイドラインに沿って行動しなければなりません。データ輸入者は、法的に許される範囲で、適用される現地の労働法および法的規制に従って、合理的に適切な身元調査を実施します。

従業員は機密保持契約を履行し、データ輸入者の機密性およびプライバシーポリシーの受領およびその遵守を確認しなければなりません。従業員はセキュリティ研修を受講します。顧客データを扱う従業員は、自らの役割に適した追加要件（例：認定）を満たさなければなりません。データ輸入者の従業員は、許可なく顧客データを処理しません。

**5. 復処理者に関するセキュリティ**

データ輸入者は、復処理者を受け入れる前に、復処理者のセキュリティおよびプライバシープラクティスの監査を実施し、復処理者がデータへのアクセス権および提供するサービスの範囲に相応しいレベルのセキュリティおよびプライバシーを提供していることを確認します。データ輸入者が復処理者によって提示されたリスクを評価した後、復処理者はセキュリティ、機密性およびプライバシーに関する適切な契約条件に同意しなければなりません。