# 取引業者のプライバシーに関する基準

## 1. 目的

**本取引業者のプライバシーに関する基準**（または「**本基準**」という。）は、**取引業者**が**リリー**とその関連会社（総称して「**リリー**」）のために**処理**する**個人情報**の秘密保持およびプライバシー要件を定めている。その目的は、**取引業者**による**処理**が、適用されるプライバシーおよびデータ保護に関する法律を全世界において遵守する事、ならびに、**リリー**の**グローバル・プライバシー・プログラム**の要件に準拠する事を、徹底することである。

## 2. 定義

**本基準**において、太字で表記した用語は、定義された用語であり、下記に定義する他、**本基準**中において適宜定義する。

(a) 「**本契約**」とは、当該契約に定義される通り、**本基準**を含むものをいう。

(b) 「**適用法**」とは、制定法、法、条約、規則、規約、条例、規制、許可、判決、命令、差止命令、令状、指令、または政府機関の類似の措置であって、文脈により、一方当事者、一方当事者の関係会社（もしあれば）、当事者の下請業者（もしあれば）またはそれらの代表者による**本契約**および**本基準**に基づく義務または行為の履行に適用されるものをいう。**適用法**は、文脈により、以下を含む。A) 1996 年医療保険の携行性と責任に関する法律（HIPAA 法）、経済的および臨床的健全性のための医療情報技術（HITECH）に関する法律、ならびに HIPAA 法および HITECH 法のすべての修正および追加の規則（総称して「**HIPAA**」）、B)欧州議会および欧州委員会規則（EU）2016/679（一般データ保護規則）、および、任意の EU 加盟国により、その権限に基づき制定された、実施、派生、または関連する国の法令、規則、または規定、ならびに（C）カリフォルニア州消費者プライバシー法 2018（CCPA 法）および同法律または類似の法律の実施に関する規則または規制のことをいう。

(c) 「**同意**」とは、自身の個人情報の処理について、情報提供を受けた上で、当該処理に対する合意を言明または明確な積極的行動により示す、個人による自発的かつ具体的な意思表示を指す。

(d) 「**データ主体**」とは、特定されたまたは特定可能な自然人をいい、特定可能な自然人とは、特に名前、識別番号、位置情報、オンラインＩＤまたは当該自然人の身体的、生理的、遺伝的、精神的、経済的、文化的もしくは社会的特定に固有な１つ以上の要素を参照することにより、直接的または間接的に特定できる者をいう。

(e) 「**データ移転プログラム**」とは、欧州経済領域（「**EEA**」）またはスイスから米国に個人情報を合法的に移転するために、欧州委員会および／またはスイス連邦委員会で承認されたフレームワークを意味する。

(f) 「**個人情報**」とは、**リリー**が提供するか、または**リリー**のために**取引業者**が収集する**データ主体**に関する情報であって、消費者または世帯に関連付けることが出来るものをいう。**個人情報**は、あらゆる媒体または形態（コンピューター化された記録または電子記録および書面のファイルを含む）で存在しうる。**個人情報**は、以下を含むがそれらに限られないものとする。(i) 姓、名もしくはイニシャル、(ii) 自宅住所その他実際の住所、(iii) 電子メール・アドレスその他のオンライン連絡先、(iv) 電話番号、(v) 社会保障番号、納税者番号、日本のマイナンバー（社会保障・税番号）、その他政府発行の識別番号等、(vi)インターネット・プロトコル（「**IP**」）アドレスもしくはホスト名、(vii) 個人を識別する他の利用可能なデータと組み合わせて継続的に使われる識別子（「**クッキー**」に保存され

ている顧客番号もしくはプロセッサー・シリアル・ナンバー）、(viii) 生年月日もしくは治療日、または (ix) **個人情報**に由来する符号化データ。
さらに、他の情報（症例報告書情報、臨床試験識別コード、個人的プロファイル情報、他の一意の識別子またはバイオメトリック情報を含むがこれらに限定されない）が処理される場合、かかる情報も**個人情報**とみなされる。なお、仮名化された**個人情報**（追加情報がなければ個人を特定できない情報）も**個人情報**とみなされる。

(g) 「**個人情報**の**処理**」（または「**処理**」）は、自動的手段であるか否かを問わず、**個人情報**について行われる操作もしくは一連の操作（収集、記録、編成、保管、改作もしくは修正、検索、参考、使用、送信による開示、配付、構造化、制限もしくは提供、配置もしくは組み合わせ、遮断もしくは消去、または破棄を含むが、これらに限られない。）を意味する。

(h) 「**個人データ侵害**」とは、移転、保管あるいは他の方法で**処理**された**個人情報**の、偶発的な、あるいは不法な破壊、紛失、改変、認められていない開示となったり、**個人情報**へのアクセスを許してしまうセキュリティ侵害をいう。

(i) 「**プライバシーに関する要請**」とは、**取引業者**が、個人または**リリー・取引業者**間の**本契約**の当事者でない団体から受領した**個人情報**に関する要請をいう。

(j) 「**センシティブ（機微な）個人情報**」とは、**個人情報**の一部分であり、その性質上、法または**リリー**の方針により、追加的にプライバシーおよびセキュリティ保護を受けるに足るものとして分類されたものをいう。**センシティブ（機微な）個人情報**は、以下を含むがこれらに限らないものとする。

(i) 政府発行のすべての識別番号。

(ii) 金融口座番号および口座ログイン認証情報。

(iii) 個人の医療記録およびバイオメトリック情報（労働者または消費者の健康、身体障害、疾病または製品に対する関心に関する情報を含む）ならびに個人の健康に関するすべてのデータ。

(iv) 直接的または間接的に、識別されたまたは識別可能な個人のものであると考えられる生物学的サンプル（組織、血液、尿その他のサンプル等）に由来する健康診断情報、健康情報または遺伝情報。

(v) 個人の身元調査報告、および米国消費者報告機関から取得したもので、米国の公正信用報告法が適用される他のすべてのデータ。

(vi) 人種、民族的背景、国籍、宗教、哲学的信条、労働組合の組合員資格の有無、政治的志向、性生活もしくは性的指向、犯罪歴、起訴もしくは有罪判決等の履歴または犯罪疑惑といった事項、を明らかにするデータ要素。

(vii) その他**リリー**が**センシティブ（機微な）個人情報**に指定する**個人情報**。例えば（但し、限定されるわけではないが）、日本の個人情報保護法で定義され、規定されている「要配慮個人情報」は、**センシティブ（機微な）個人情報**に含まれる。

(k) 「**本サービス**」とは、**本契約**に基づき**取引業者**が**リリー**のために行う特定の業務を意味する。

  

(l)　「**標準契約条項（SCC）**」とは、EEA 加盟国およびスイス外の、欧州委員会がデータ保護のレベルが不十分であると見做す国において設立された処理業者への個人情報移転について規制する、欧州委員会発行の指令 95/46/EC の第 26 条第 2 項により要求される契約条項をいう。

**3.　一般的義務**

(a)　**本契約**に基づく**取引業者**のすべての義務は、**本基準**の要件に追加されるものである。**取引業者**は、**リリー**のためおよび**リリー**の書面による指示に従って**本サービス**を履行する以外のいかなる目的にも、**個人情報**の**処理**、保持、開示を行わず、その他**個人情報**を使用しないものとする。その**処理**等には、第三国や国際的な組織への**個人情報**の移転に関する事も含む。目的外の**処理**等は、**取引業者**が対象となっている**適用法**によって要求されない限り、行ってはならない。法の要求に基づき**処理**する場合、その法が公益上の重要な理由に基づき通知を禁止しない限り、**取引業者**は、**処理**する前に、**リリー**に法律上要求されている旨を通知する。**本基準**の要件を完全に遵守すると、**本契約**に基づく他の義務を履行することができないと**取引業者**が信ずる場合、**取引業者**は、**本契約**の通知条項に従って、直ちに**リリー**に通知し、矛盾が解消されるまで、**本基準**に違反するようないかなる行為にも着手しないものとする。

(b)　適切な間隔をおいて、あるいは**リリー**からの要求に基づき、**取引業者**はプライバシーポリシーと手順書の写しを**リリー**に提供するものとする。

(c)　**取引業者**は、以下の場合は直ちに（72 時間以内に）、**プライバシーに関する要請**を電子メール（privacy@lilly.com）を通じ書面で**リリー**に通知する。

1.　**データ主体**である（または**データ主体**であると主張する）個人から、**取引業者**が受領した**個人情報**の閲覧を求める要請を受けた場合や、**データ主体**から当該**個人情報**の**処理**を中止することや、当該**個人情報**の修正、アクセス拒否、消去もしくは破棄を求める要請を受けた場合など、**データ主体**から、**適用法**上の権利に基づく要請を受けた場合。

2.　構造化された、一般的に使用されるコンピュータが読み取り可能な形式で**個人情報**の開示を受けたい旨の要請、および／または**個人情報**を第三者へ移転してもらいたい旨の要請を**データ主体**から受けた場合。

3.　**取引業者**が受領した**個人情報**について、政府職員（データ保護機関または法執行機関を含む）から閲覧を求める要請、当該**個人情報**の**処理**を中止するもしくは開始しないこと求める要請、または政府職員から当該**個人情報**の修正、アクセス拒否、消去もしくは破棄を求める要請を受けた場合。

4.　**取引業者**が受領した**個人情報**の**処理**に関して照会、請求または苦情を受けた場合。

**データ主体**であると主張する個人からの**プライバシーに関する要請**を受領した場合、取引業者は合理的な努力を尽くし、当該個人が**データ主体**であるか否かを確認する。

**適用法**に基づき**取引業者**に開示を強制する召喚令状または類似の法的文書により政府機関又は第三者から要請を受けた場合を除き、**取引業者**は、**本契約**によりまたは**リリー**の書面により明示的に許可されない限り、**プライバシーに関する要請**に応じることが許可されないことを了解する。

適用法で認められる最大の範囲で、**取引業者**は、自己の費用負担で、直ちにかかる**プライバシーに関する要請**を**リリー**に開示し、**リリー**が合理的に要請するすべての支援を提供し、**プライバシーに関する要請**への対応につき**リリー**の指示に従う。**リリー**が**プライバシーに関する要請**を受けた場合、リリ

ーの要請に応じて、**取引業者**は直ちに**リリー**にすべての情報を提供し、**リリー**が合理的に要請する支援を提供すると共に、かかる**プライバシーに関する要請**つき**リリー**の合理的な指示に従う。.

(d) **取引業者**は、**本基準**の違反になりうると認知した**個人データ侵害**あるいは**個人情報**の使用や開示に関する通報について、直ちに徹底した調査を実施する。**個人データ侵害**や重大な**本基準**違反の疑いを発見した場合、**取引業者**は速やかに（24 時間以内に）**リリー**に電子メール（privacy@lilly.com）で通知する。さらに上記に関連して、**取引業者**は潜在的損害を軽減するため**リリー**を合理的範囲で支援し、根本的原因を分析し、さらに**リリー**の要請に応じて分析結果および是正計画を**リリー**と共有する。取引業者は、**個人データ侵害**や**本基準**違反への対応にかかる全費用（調査実施費用、**適用法**、その他の適用される規制、ガイドラインまたは基準において必要な消費者およびその他の者への通知費用、一年間の信用モニターを消費者に提供する費用、消費者、規制担当者及びメディアからの問合せへの対応費用を含むが、これらに限られない。）を負担する。

(e) 契約した**本サービス**を履行する際に**取引業者**が収集またはアクセスする**個人情報**は、**本サービス**を履行するためまたは法的要件を満たすために必要なものに限定されるものとする。**取引業者**は、**本契約**及び/又は個別発注書に記載した**本サービス**または事業の利用目的の達成に必要な限度に限り、**個人情報**の**処理**を行うものとする。**本サービス**もしくは当該利用目的の達成または法律上の義務に必要な期間に限り、**個人情報**を保管するものとする。**取引業者**は、**本契約**の文書管理条項に従い、**個人情報**の完全性および通用性を確保するために適正な措置を講じるものとする。

(f) **本サービス**が**個人情報**を**データ主体**から直接（例えば、登録手続きまたはウェブページを通して）収集することを必要とする場合、**取引業者**は、各**データ主体**に予め**個人情報**の利用に関する明瞭かつ明白で、簡潔、平明で、分かりやすくかつ容易に入手可能な通知（**個人情報**の利用目的を含むものとする）を行う。通知は、**本契約**の規定および**リリー**の指示に沿ったものでなければならない。**取引業者**による**データ主体**からの直接の**個人情報**の収集が、日本の個人情報保護法で定義され規定されている要配慮個人情報の収集を行う場合、**取引業者**は、予め本人の**同意**を得なければならない。**センシティブ（機微な）個人情報**の取得にあたって、別途特に**リリー**が要求した場合、または**本契約**もしくは**適用法**で義務づけられている場合、**取引業者**は**データ主体**から**同意**を取得する。ただし、**取引業者**がウェブページその他の方法で使用条件、プライバシー・ステイトメントその他の条項を**データ主体**に提示したとしても、**本基準**に基づく**取引業者**の義務もしくは権利または**取引業者**が**個人情報**を使用できる方法は一切変更されないものとする。

(g) **取引業者**は、国境を越えて**個人情報**を移転してはならず、**個人情報**への遠隔アクセスを従業員、関連会社、請負業者、サービス提供者その他第三者に許可してはならない。ただし、**リリー**が**取引業者**に提供する**処理**の指示書において、かかる国境を越える**個人情報**の移転または遠隔アクセスが明示的に許可されている場合、または当該移転もしくは遠隔アクセスについて**リリー**の事前の書面による**同意**を得ている場合はこの限りではない。**取引業者**は、**適用法**により必要となりうる遵守体制を整備し、実行することに**同意**し、**取引業者**が**個人情報**をかかる国から受け取る、またはかかる国に送付できるようにする。

上記事項に影響を及ぼすことなく、**取引業者**は、**本契約**において、EEA加盟国またはスイスから、欧州委員会によって適切なデータ保護を提供すると見なされていない国へ**個人情報**を移転する場合、以下を行わなければならない。

1. 個人情報の **EEA** および／もしくはスイスから**取引業者**への移転または、場合により、取引業者による **EEA** および／もしくはスイスの個人情報への遠隔アクセスのすべてについて、欧州委員会によって規定された**標準契約条項（SCC）**（その修正を含む）を締結して**本契**

**約**に付属させる。**取引業者**は、**個人情報**を **SCC** に従って**処理**し、“データ輸入者”（または場合によっては“復処理者”）に課せられる義務を履行する。**取引業者**は、**標準契約条項**における受益権を適切な第三者に与える。**取引業者**は、いかなる理由であれ、**SCC** で要求されるのと同等の保護の基準を達成できないと合理的に判断した場合、**リリー**に対し速やかにその判断を書面によって通知し、かかる**処理**を速やかに修正し、修正が不能な場合には、当該**個人情報**に関する一切の**処理**を停止する。

2. **SCC** がデータ移転方法として利用することが出来ず、取引業者が**データ移転プログラム**において認定されている場合、この**取引業者**は (a) 当該認定に、**本契約**で定められた**取引業者**による**本サービス**、および**個人情報**に対する意図された**処理**が含まれていること、および (b) **取引業者**が**個人情報**を**処理**している期間、かかる**データ移転プログラム**において、**取引業者**が認定された状態であることを保証する。または、

3. 何らかの理由で、**取引業者**が前述の第 1 号または第 2 号を遵守できない場合、**取引業者**は直ちに**リリー**に通知する。両当事者は、直ちに協力して、適切な代替の移転および遵守方法を決定し実施するものとする。

すべての場合において、各当事者は、当該移転および遵守方法の決定および維持に関して発生する自己の費用を負担するものとする。**リリー**および**取引業者**は、相互の書面合意により、データ移転契約その他遵守方法を終了または変更することができる。

(h) **リリー**は通常、**取引業者**が**個人情報**の**処理**を下請業者に再委託することを許可するが、この場合、**取引業者**が**リリー**に対し、下請業者を追加したり入れ替える際に変更予定を通知することを条件とし、**リリー**はかかる変更に異議を唱え、両当事者が下請業者について合意できない場合には、**本契約**を解除する権利を留保する。下請業者には、**本契約**の下で**取引業者**が提供することになっている**本サービス**を履行するためにのみ**個人情報**を**処理**することが認められ、それ以外のいかなる目的でも**個人情報**を**処理**することは禁止される。下請業者に**個人情報**へのアクセス権を付与するに先立ち、**取引業者**は、かかる下請業者に**本契約**と同程度の保護条件の遵守を義務づける契約書を交わさなければならない。**取引業者**は、下請業者の作為または不作為について、**取引業者**自身による作為または不作為の場合と同等に全面的な責任を負う。

(i) **本契約**の**取引業者**の義務に関する規定に影響を及ぼすことなく、**取引業者**は、**リリー**と協力して、**個人情報**の**処理**に関する照会、請求、苦情および要求（削除要求を含む。）に対応するものとする。

(j) **取引業者**は、その従業員および承認された下請業者から、すべての必要な許可を確保して、**リリー**が、**本契約**を履行するために必要とするかかる個人の**個人情報**（**リリー**のシステムまたは施設にアクセスするために必要な情報、個別の実績測定基準の維持および類似する情報を含む）の**処理**をできるようにする。

**4. 個人情報の秘密保持**

(a) **個人情報**は、**本契約**における**個人情報**とみなされ、**取引業者**は、すべての**本契約**の履行のために**処理**された**個人情報**を、**本契約**に従って極秘に維持しなければならない。**取引業者**は、**本サービス**を履行するために**個人情報**にアクセスする必要があり、**個人情報**を秘密に保持する拘束力を有する義務を負う従業員および**取引業者**の社内で業務を行う請負業者のみに**個人情報**を提供する。**取引業者**

  

は、**リリー**が 3(h)によって明示的に開示、送信または提供を許可しない限り、**個人情報**を第三者（下請業者を含む）に開示、送信または提供してはならない。

(b) **取引業者**が**リリー**のための**本サービス**の履行を中止する場合、**取引業者**は、**リリー**の選択に従い、すべての**個人情報**（**個人情報**を含む全ての写しおよび全ての媒体と共に）を**リリー**に返却するか、または全ての**個人情報**を安全に破棄し、その旨を**リリー**に証明する。

**5. セキュリティ**

(a) **取引業者**は、**本契約**の一部である**リリー**の情報セキュリティ基準（ISS）に従い、偶発的もしくは不法な破損、改変または無許可の開示もしくはアクセスから**個人情報**を保護するために、適切で実行可能な、技術的および組織的な方策を文書化し、実施していなければならない。**取引業者**は、安全手段の管理、システムおよび手順の有効性および耐性（レジリエンス）を定期的に試験し、その他監視する。**取引業者**は、**個人情報**のセキュリティ、秘密保持、可用性および完全性に対して合理的に予見できる内外のリスクを定期的に特定し、かかるリスクを制御するための安全手段が適切に講じられているよう徹底する（**個人情報**の仮名化および暗号化を含む）。 **適用法**に従って、**取引業者**は、セキュリティ・プログラムの要件を遵守するために従業員および下請業者を監視するものとする。

(b) **取引業者**は、**本契約**を遵守していることを証明するために、そして**本契約**に従って**取引業者**の**個人情報**の**処理**に関する**適用法**により求められているように、必要な全ての文書を保持するものとする。**リリー**の要請に応じて、**取引業者**は、そのデータ**処理**施設を、**リリー**の監査対象とするものとする。監査は、**リリー**（または**リリー**が選択する独立検査会社）により実施されるものとする。**取引業者**は、**取引業者**の経費負担にて当該監査に十分に協力するものとする。当該監査により、**取引業者**のセキュリティ計画に重大な欠陥または弱点があることが明らかになったり、**本契約**違反が明らかになった場合、**リリー**は、かかる問題が解決されるまで**取引業者**への**個人情報**の送信を停止し、**取引業者**による当該**個人情報**の**処理**を停止させる権利を有するものとするが、これにより**リリー**の他の権利に影響を与えるものではない。さらに、**取引業者**のセキュリティプログラムにおける欠陥に対応する、あるいは違反を是正し再発を防止するため必要な変更を、**取引業者**は自己の経費と出費で直ちに実施する。

**6. 法律の遵守**

(a) **取引業者**は、**個人情報**の**処理**のための法律上の要件および監督機関の要件について精通していなければならない。**取引業者**は、**本サービス**の為に**処理**を行うだけではなく、**処理**にあたり全ての**適用法**を遵守していなければならない。

(b) **取引業者**は、政府機関、規制当局および監督当局への協力、ならびにデータ保護影響評価への協力を含め、**リリー**が**適用法**を遵守できるよう、直ちに**リリー**を支援し、協力する。

(c) **適用法**により義務づけられている場合、**取引業者**はデータ保護責任者を任命し、同責任者の氏名および連絡先情報を**リリー**に連絡し、同責任者に変更があれば常に**リリー**に通知しなければならない。

**7. 責任／補償**

**取引業者**が**本基準**に違反した場合、それによって生じた責任、損失、請求、損害、費用（合理的な弁護士費用を含む。）について、**リリー**を補償し、**リリー**を免責する。これには、**本契約**によって想定

  

された以外の**個人情報**の使用によって生じる第三者への支払いも含むが、これに限られない。**本契約**の他の条項にかかわらず、**本基準**に違反する**個人情報**の収集、使用、開示または保持については、責任の排除や限定は認められないものとする。

**別紙 A**
**データ処理に関する情報**
**（取引業者が EEA 加盟国またはスイスからの個人情報を処理する場合にのみ使用）**
（取引業者が記入しリリーに返送）

**取引業者**は、知りうる限りにおいて、以下の記載が正確であることを表明する。

1. **取引業者**の商号、本店所在地

2. **本サービス**において規定された**取引業者**が行うデータ**処理**の趣旨及び目的

3. **本サービス**において**取引業者**が**処理**する**データ主体**に基づくデータの分類（以下から選択）

- ☐ 従業員データ
- ☐ 消費者データ
- ☐ 医療提供者（Healthcare Provider）データ
- ☐ 動物医療提供者（Animal Healthcare Provider）データ
- ☐ 治験参加者データ
- ☐ 治験担当医師データ
- ☐ 取引業者または他の事業者の従業員データ
- ☐ その他処理される個人情報（具体的に記載）

4. **本サービス**において**取引業者**が処理する**リリー**の情報（以下から選択）

- ☐ 顧客および取引先ならびにそれらの担当者に関する以下のデータ：名前、会社、所在地、担当者、連絡先、優先または除外連絡先、希望の情報およびニュースレター、発送、運送および支払い条件、会計顧問、活動情報、イベントへ参加状況、キャンペーン情報、顧客満足、顧客評価スコアならびに見込み顧客

- ☐ 医療従事者（ソートリーダーを含む）に関する以下のデータ：名前、機関、所在地、担当者、連絡先、学歴、専門分野、能力および経験等の職務経歴、治験または臨床研究における協力内容、想定される利益相反、イベントへの参加状況、支払い条件

- ☐ ウェブサイト訪問者に関する以下のデータ：IP アドレス、訪問日時、訪問されたページ、訪問経緯、訪問者が使用するブラウザ、訪問者が使用する OS、訪問者のプロバイダのドメインネームおよびアドレスならびに（場合によっては）訪問者が手動で入力したデータ

- ☐ **リリー**の従業員（従業員、フリーランス、役員を含む）に関する以下のデータ：職務経歴書上のデータ、給与口座データ、研修および業績管理に関するデータ、企業年金に関するデータ、有給取得回数、欠勤回数、通勤手当、運転免許に関するデータ、業務中の事故、システムログに関するデータおよびその他収集される可能性がある人事情報

- ☐ 患者に関する以下のデータ：患者の健康状態を含む患者総合データ、薬物に関する情報、患者サポートプログラムに関する情報、有害事象通知、苦情等に関する情報

- ☐ 取引の相手方、特に担当者との情報交換に関する情報：電子メール、ファクシミリ、電話の通信データ、電子メール、ファクシミリ、郵便物の内容

  

- ☐ アンケートやマーケットリサーチ等のデータおよび結果：アカウントおよびサブアカウント（連絡先、担当者、活動、発送、運搬および支払い条件など）、処理業者の責任者

- ☐ 契約のマスターデータ、価格、特約、注文、配送データ、請求書データ、支払いデータ、銀行口座データ、支払残高に関するデータ、およびそれらの履歴

- ☐ 個々の取引先、顧客、潜在的顧客および取引先とのビジネス上の文書および関連履歴、契約、アカウント、またはシステム上に保存されたその他のデータの記録

- ☐ **リリー**によって提供されたサービスの使用によって生じたデータ（使用履歴等から生じる個人識別票など）

5. **取引業者**が**個人情報**の**処理**を行う地域（**処理**業務を行う国を記載）