取引業者のプライバシーとセキュリティに関する基準

1. 目的

本取引業者・プライバシー基準（または「**本基準**」という。）は、**取引業者**がリリーのために**処理**する**個人情報**の秘密保持、セキュリティ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、セキュリティ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、イーライリリーの**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、**取引業者**がリリーのために業務を実施する際の基準となる、**取引業者**とリリー間の契約全体を意味する。**本契約**の成立は、両当事者が契約書に署名することにより、リリーの購入注文を**取引業者**が明示的もしくは黙示的に承諾することにより、またはその他の方法による契約の申込と承諾により実現する。

(b) 「**適用法**」とは、制定法、法、条約、規則、規約、条例、規制、許可、解釈、認証、判決、命令、差止命令、令状、指令、召喚令状、または政府機関の類似の措置であって、文脈により、以下に適用されるものを意味する。(i)**本契約**および**本基準**、(ii) **本契約**に関する義務の履行その他の行為、ならびに (iii)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。**適用法**は以下を含む。A) 1996 年医療保険の携行性と責任に関する法律（HIPAA 法）、B) 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、HIPAA のプライバシーとセキュリティ・ルールの規則、HITECH 法および遺伝情報差別禁止法に基づく HIPAA プライバシー、セキュリティ、執行および違反通知ルールに対する修正（「**総括的最終規則**」）、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**」）、C) 適宜、修正、更新、または撤回された個人データ処理に係る個人の保護及び当該データの自由な移動に関する 1995 年 10 月 24 日付欧州議会及び理事会の指令 95/46/EC（「**指令**」）、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、並びに、適用可能となった場合は欧州一般データ保護規則（規則（EU）2016/679）のことをいう。

(c) 「**データ移転プログラム**」とは、プライバシーシールド、スイス・米国間セーフハーバーなど、**指令**の第25(6)条に準じた適切な保護レベルを提供するものとして欧州委員会により承認された、欧州経済領域(「**EEA**」)またはスイスから米国に個人情報を移転するためのフレームワークを意味する。

(d) 「**個人情報**」とは、リリーおよび／もしくはその関連会社が提供するか、またはリリーおよび／もしくはその関連会社のために**取引業者**が収集する情報であって、(i) 個人を特定する情報、またはリリーが提供する他の情報もしくはリリーのために**取引業者**が**処理**をする他の情報と組み合わせて使用した場合に、個人を特定する情報、または、(ii) 個人の識別情報もしくは連絡先を引き出すことができる情報を意味する。**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。(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（市町村名および通り名を含む）、(iii) 電子メール・アドレスその他のオンライン連絡先（個人の電子メール・アドレスを記載したインスタント・メッセージのユーザー識別子またはツイッター等で使用する通称等）、(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）、運転免許証番号、その他政府発行の識別番号

等、(vi) 個人を識別するインターネット・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られる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、IPアドレス、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**個人情報**に関連づけられるか、組み合わせられる場合、かかる情報も**個人情報**とみなされる。最初にアメリカ合衆国で収集されたデータに関しては、**個人情報**には、リリーの従業員個人の氏名、勤務先電話番号、勤務先携帯電話番号、勤務先住所、勤務先電子メール・アドレスまたはリリー内部の識別番号は含まないものとする。

(e) 「**プライバシーシールド**」とは、2016年2月2日に合意され、2016年7月12日、欧州委員会実施決定C(2016) 4176により正式採択されたプライバシー原則のEU・米国間フレームワークである。

(f) 「**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（例えば、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、配付もしくは提供、配置もしくは組み合わせ、遮断もしくは分散消去、または破棄）を意味する。

(g) 「**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。

(i) 政府発行のすべての識別番号（米国の社会保障番号（SSN）、欧州連合の社会保障番号（SSN）、カナダの社会保険番号（SIN）、日本のマイナンバー（社会保障・税番号）、運転免許証番号および旅券番号を含む）。

(ii) 金融口座番号（銀行口座番号、クレジットカード番号、その他により金融口座へのアクセスが可能になるような情報）。

(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、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、センシティブ個人情報に含まれる。

(h) 「**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。

(i)　「含んでいる」、「含む」もしくは「特に」またはそれらに類似する用語の後にくる文言は、例示と解釈されるものとし、これらの用語の前の文言、説明、定義，句または用語の意味を制限しないものとする。

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（性質上類似するものを含む）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指示に従って**本サービス**を遂行する以外のいかなる目的にも、**個人情報**の**処理**を行わず、その他**個人情報**を使用しないものとする。**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、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)　**取引業者**は、以下の場合は直ちに書面でリリーに通知する。

(i)　データの主体である（または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**について、閲覧を求める要請、当該**個人情報**の**処理**を中止もしくは開始しないことを求める要請、または個人から当該**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。

(ii)　**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。

(iii)　**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。

(iv)　リリーの従業員その他第三者から受領した**個人情報**に関するその他の要請を受けた場合。ただし、合意書に記載されている要請、かかる**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除く。

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る政府機関から受けた要請を除き、**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、かかる要請に応じることが許可されないことを了解する。

(c)　契約した**本サービス**を遂行する際に**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**を遂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**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。

(d)　**本サービス**が**個人情報**を個人から直接（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、予め**個人情報**の使用に関する明瞭かつ明白な通知（**個人情報**の利用目的を含むものとする）を行う。**本サービス**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。当該通知は、**取引業者**とリリー間の合意書の条項に一致しているものとする。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個人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。

(e) **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、リリーまたはその関連会社に適用される適用法（の加盟国のいずれかおよびスイスのデータ保護法を含む）により必要となりうる遵守方策を作成し、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、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の国内で、**EEA**加盟国またはスイスから直接、**個人情報**を受け取る前に、以下を行わなければならない。

(i) リリーまたはその関係会社と直ちに協力して、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**（**データ移転に関する EU 標準契約条項**）を正式に作成し、締結し、遵守する。または、

(ii) 前記に拘わらず、**データ移転プログラム**で認定されている**取引業者**が、米国内で **EEA** 加盟国またはスイスから**個人情報**を受け取る場合、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、(b) **取引業者**が**個人情報**を**処理**している間、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、および (c) **取引業者**が**個人情報**を**処理**している間、いかなる時でも、**取引業者**が認定を取り消された、または当該認定を失った、または何らかの理由で**データ移転プログラム**が効力を失った場合には、**取引業者**は前述の第(i)号に従うことを保証する。または、

(iii) 何らかの理由で、**取引業者**が前述の第(i)号または第(ii)号を遵守できない場合、**両当事者**は、直ちに協力して、適切な代替の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。**EEA**またはスイスからのデータ移転について、当該国（またはその国の関連セクター）に関して発布されている**指令**の第25(6)条（またはそれに代わる法律）に基づく欧州委員会の肯定的十分性決定により、データ移転契約その他遵守方法が不必要になる、または**指令**95/46/EC（またはそれに代わる法律）が当該国において直接適用されるようになる場合、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。ただし、取引業者は、その十分性決定から利益を得るために必要とされる自己認証その他の必要な処置を最初に講じるものとする。

取引業者が、**EEA**またはスイスを出所とする**個人情報**をリリーまたはデータ移転プログラムの認定を受けているリリーの米国関係法人から受け取った場合、この**取引業者**は、かかる**個人情報**を、**データ移転プログラム**と一致した方法で、**データ移転プログラム**と同じレベルの保護を提供しながら処理しなければならない。**取引業者**が、理由の如何にかかわらず、**データ移転プログラム**と同じレベルの保護を提供できないと合理的に判断した場合、この**取引業者**は、直ちにかかる判断をリリーに書面で通知し、速やかにかかる**処理**を修正するか、それが不可能であれば、かかる**個人情報**のいかなる**処理**も中止しなければならない。

(f) **取引業者**から第三者への**個人情報**の移転またはアクセスが許可されている場合、**取引業者**は、当該第三者との間で書面合意を締結したときのみ、これを実行することを約束する。当該合意は、**本基準**に基づき**取引業者**に課される義務（第3条(e)項に定められた義務を含む）と同じ義務を第三者に課すものとする。

取引業者による上記の条項 3(e) および／または 3(f) の違反は、**取引業者**による**本契約**の重大な違反とみなされ、リリーは、直ちに両当事者間の**本契約**を解除することができるものとする。リリーは、**本契約**を解除することを選択した場合、**取引業者**に通知を行うものとする（**本契約**に通知条項がある場合には、当該通知条項の定めに従い通知するものとする）。

(g) **取引業者**は、リリーならびにリリーの関係会社および代表者に協力して、**個人情報**の**処理**に関する照会、請求および苦情に対応するものとする。

(h) **取引業者**は、すべての必要な許可をその従業員および承認された下請業者から確保して、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**ができるようにする。

(i) **本契約**にこれと異なる定めがあることにかかわらず、(a) **本基準**により明示的に許可されているリリーによる行為は、リリーによる**本契約**の違反とならず、(b) 当該行為により**本契約**に基づく**取引業者**の履行が免除されることは一切ない。

4. 個人情報の秘密保持

(a) **取引業者**は、すべての**個人情報**を極秘に維持しなければならない。**取引業者**は、**本サービス**を遂行するために**個人情報**にアクセスする必要がある従業員および**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、リリーが書面により明示的に開示、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。いかなる場合も、**取引業者**は、下請取引業者または取引業者から委託されて処理する者が本書に記載する条件（セキュリティおよびリリーの監査権に関する条項を含む）に書面で同意していない限り、**個人情報**（または他のリリーの情報）を下請取引業者または下請処理者に提供することはできない。

(b) **取引業者**がリリーのための**本サービス**の遂行を中止する場合、**取引業者**は、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**を確実に破棄し、その旨をリリーに証明する。（**取引業者**に適用される法により、移転された**個人情報**の全てまたは一部を破棄することが許可されない場合、**取引業者**は、**個人情報**の秘密保持およびセキュリティを引き続き徹底すること、ならびに移転された**個人情報**を取引関係終了後に能動的に**処理**しないことを保証する。）

5. セキュリティ

(a) **取引業者**は、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、実施しているものとする。**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チェック・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。**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

よび請負業者を監視するものとする。

(b) 適切な間隔を置いてまたは別途リリーの要求に従い、**取引業者**は、書面によるプライバシーならびに情報セキュリティ方針および手順の写しをリリーに提供する。

(c) 従業員または請負業者に**個人情報**の**処理**を許可する前に、**取引業者**は、(i)従業員個人または請負業者個人の適切な身元調査を行い、(ii) 法的に有効な秘密保持契約を締結するようかかる個人に義務付け、ならびに (iii)プライバシーおよびセキュリティに関する適切な研修をかかる個人に受けさせるものとする。要求があれば、**取引業者**は、**個人情報**にアクセスできる（またはアクセスできた）全ての従業員および請負業者（元従業員および元請負業者を含む）のリストをリリーに提供するものとする。

(d) **処理**のためにネットワーク上で**個人情報**を送信する必要がある場合、**取引業者**は、**処理**によってもたらされる特定のリスクから**個人情報**を保護するための適切な、そのような**処理**に対応した補完的手段を実施しているものとする。**センシティブ（機微な）個人情報**は、暗号化されたフォーマットでのみ送信することができる。

(e) **処理**のために**取引業者**の施設または**取引業者**が管理するコンピューター・システムで**個人情報**を取り扱う必要がある場合、**取引業者**は、以下の具体的な基準を遵守するものとする。

(i) アクセス権：**取引業者**は、アクセス権を管理するために有効な手順を設けるものとする。この手順には、次の管理手順が含まれる。1. コンピュータ・システムのユーザーおよびシステム資源は、それぞれ求められている機能を実行するために必要なアクセス権のみが与えられ、2. アクセス権は、人員またはシステムの変更に基づいて更新され、ならびに 3. アクセス権は、アプリケーションまたはシステムへのリスクに基づき、適切な頻度で定期的に見直されるものとする。**取引業者**は、リスクのレベルに応じた有効な認証方法も用いるものとする。

(ii) アクセス手続き：**取引業者**は、下記を実行するものとする。

1. 悪意のあるまたは無許可の人々による物理的侵害、環境汚染物質による損傷、および能動的もしくは受動的電子放出による電子的侵害のリスクから保護するために、物理的セキュリティ区画の設定、ならびに各区画における適切な予防的コントロールおよび発見的コントロールの実施。

2. 無許可のアクセスから保護するための複数のアクセス制御を用いたコンピューター・ネットワークの保護。特に、**取引業者**は、(i) ネットワーク・サーバー、アプリケーション、データおよびユーザーをセキュリティ領域に分類し、(ii) 各セキュリティ領域内および各セキュリティ領域間に、適切なアクセス要件を設定し、(iii)適切な技術的管理（例えば、ファイアウォールを含む）を実施して、アクセス要件を一貫して満たすものとする。

3. オペレーティング・システムおよびアプリケーションへのアクセスのセキュリティ対策。**取引業者**は、業務上の必要性が一切ない場合にはオペレーティング・システム・レベルで遠隔通信を無効にすることにより、ならびに／またはマネジメント承認、ロバスト制御、アクセス・イベントのロギングおよびモニタリング、ならびにその後の監査を通じてアクセスを厳しく制御することにより、かかるシステムとの間の遠隔アクセスのセキュリティ対策を行うものとする。

(iii) 悪質なコード： **取引業者**は、悪質なコードのリスクを防ぐために、クライアント*) およびサーバーでアンチウィルス製品を用い、ネットワーク周辺に適切なブロッキング策を施し、アプリケーションへの入力をフィルタリング処理し、ならびに適切なコンピューター方針および慣行を策定し、実施し、スタッフの研修を行うものとする。
（＊親システム (server) に要求を出して処理をしてもらうシステム。）

(iv) 媒体の取り扱い： **取引業者**は、損失または損害を回避するために、紙、フィルムおよびコンピューター・ベースの媒体へのアクセスを制御し保護するものとする。特に、**センシティブ（機微な）個人情報**を含んでいる全ての媒体について、**取引業者**は、当該媒体の安全かつ確実な処分を徹底し、第三者への移転または送信に際してすべての媒体につきセキュリティ対策を行う。

(v) その他の管理：**取引業者**は、下記を実行するものとする。

1. システムが、適切なセキュリティ・コントロールを用いて開発、取得および維持されるよう徹底する。

2. セキュリティ・イベントのモニタリングおよびロギングを保証するシステムおよびアプリケーションを特定し、ログ・ファイルを合理的に維持および分析する。

3. (i) サービス提供者を探して選定するにあたり相当な注意を払うこと、および (ii) 秘密保持、セキュリティ責任、管理および報告に関して契約による保証をすることにより、外注した業務に対するセキュリティ責任を果たす。

4. **個人情報**への現行のアクセスに対応した障害回復／業務継続計画を確立し、また、バックアップ・サイトおよび代替通信ネットワークに対するセキュリティ上の必要性についても確保する。

5. **取引業者**は、**取引業者**、**取引業者**の従業者、又は、下請業者、下請取引業者、取引業者の委託により処理した者の故意又は過失により、個人情報に対する不正アクセス又は個人情報の紛失，破壊、改竄、漏洩等の事故（「**当該事故**」）が発生したときは、当該事故に関連してリリーの被った損害を賠償するものとする。

6. 異なる目的のために収集された**個人情報**は、分けて別に**処理**するよう徹底する。**取引業者**は、特に、**本契約**に基づきリリーおよび／またはその関連会社のために**処理**する**個人情報**を他の顧客のデータとは分けて**処理**するよう徹底する。

(f) **センシティブ（機微な）個人情報**を、ポータブル・コンピューター機器または媒体（ラップトップ・コンピューター、リムーバブル・ハードディスクもしくはフラッシュ・ドライブ、携帯端末（PDA）またはコンピューター・テープを含む）に保存してはならない。ただし、**センシティブ（機微な）個人情報**が暗号化されている場合、または**センシティブ（機微な）個人情報**を記憶するポータブル・コンピューター機器または媒体のハードディスクが完全に暗号化されている場合はこの限りではない。

(g) **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（またはリリーが指定する独立検査会社）により実施されるものとする。**取引業者**は、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。

(h) **取引業者**は、**個人情報**の使用または開示が**本基準**に違反する疑いがあることを察知した場合には、その疑いにつき直ちに徹底的に調査し、重大な違反は全て直ちに書面でリリーに通知する。**取引業者**は、**個人情報**への無許可のアクセスまたは開示を発見したときは、直ちに、リリーに通知する。**取引業者**は、セキュリティ侵害の解決に関するすべての費用を負担する。当該費用には、調査の実施、消費者その他法律またはクレジットカード情報等に関する PCI データ・セキュリティ・スタンダード*によって要求される他者への通知、消費者への 1 年間のクレジット・モニタリングの提供、ならびに消費者、監督機関およびメディアへの応答に要する費用が含まれる。
（*クレジットカード情報および取り引き情報を保護するために、JCB・American Express・Discover・マスターカード・VISA の国際ペイメントブランド 5 社が共同で策定した、クレジット業界におけるグローバルセキュリティ基準である。）

6. 法律の遵守

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。

7. EEA／スイス ― 特定の条件

(a) 別途通知されない限り、**取引業者**は、第 3(e)(i)条の下、**標準契約条項**に基づいて、**EEA** またはスイスから**取引業者**に（直接的または間接的に）移転された**個人情報**を**処理**する場合、欧州委員会によって規定され、当該**個人情報**に関して必要に応じて修正される**標準契約条項**（リリーの購買部のポータルに「**データ移転に関する EU 標準契約条項**」として記載されている）に基づき「データ輸入者」（または該当する場合、その「下請処理業者」）に課される義務を遵守しなければならない。**取引業者**は、本書を以て、**標準契約条項**に規定する該当する第三者受益権を、データ主体（下記(b)で定義する）に対して、付与する。

(b) 当該**個人情報**に関わる個人（「**データ主体**」）またはその代理として行動する者が、**標準契約条項**の違反を理由にリリーまたはその関連会社に対して請求を提起する権利を有し、当該請求が**取引業者**の**本契約**および**本基準**に基づく**処理**業務に起因する場合、**取引業者**は、当該請求に起因または関連してリリーまたはその関連会社が被るすべての債務、費用、経費、損害および損失（全額補償ベースで算出される、直接、間接もしくは派生的損害、逸失利益、評判およびすべての利権の損失、罰金および訴訟費用ならびにその他すべての合理的な専門家の費用および経費を含む）について、リリーまたはその関連会社に補償するものとする。ただし、

i. **取引業者は、**合理的に可能な限り速やかに、当該請求について通知を受け、また

ii. リリーまたは（場合により）その関連会社は、**取引業者**の書面による事前の同意（当該同意は、不合理に条件付け、保留または遅延されない）を得ずに、当該請求に関する責任の承認、合意または和解を行ってはならないものとする。ただし、当該請求を解決しなければ、何らかの重要な点において、自身に損害が及ぶとリリーまたはその関連会社が信じる場

合、リリーまたは当該関連会社は、（解決の条件を（法的に可能な範囲で）事前に書面で**取引業者**に通知した後、**取引業者**の同意を得ずに）当該請求を解決することができる。

(c) **取引業者**は、リリーまたはその関係会社の要請に応じて速やかに、別途リリーが指定する遵守書（「『取引業者のプライバシーおよびセキュリティに関する基準』の遵守について」と題する書面）の「欧州の個人情報を取扱う場合」に記入すべき箇所に記入し、リリーまたは要請元の関係会社（もしあれば）に返送するものとする。