KANTAR

この翻訳の意味と英語版との間に相違がある場合は、英語版が優先されます。

契約条件（サービスの購入）

1. **定義**

1.1 本契約において、次の各語をそれぞれ以下のとおり定義します。

1.1.1 「**本契約**」とは、発注書および本契約条件をまとめたものをいいます。

1.1.2 **「関連会社」**とは、1 社または複数の仲介業者を通じて直接的あるいは間接的に管理する、または共通の管理権によって、または共通の管理下にあり、随時 Kantar として取引を行う企業をいいます（ただし Europanel を除きます）。

1.1.3 「**秘密情報**」とは、顧客および／または Kantar グループの取締役、役員、従業員、予算、価格、注文控元帳、方法、アンケートの報告、財務、親会社および子会社、顧客データおよび顧客とそのクライアントに関連する情報をいいます。

1.1.4 **「管理」**とは以下を意味します。

(a) 議決権またはその他に関連する契約により、かかる企業の議決権のある株式持分またはその他の持ち分を通じ、直接的あるいは間接的に、かかる企業の運営または方針を指揮する権限を所有すること

(b) 直接的あるいは間接的に、かかる企業の議決権のある株式持分またはその他の持ち分の 50%を所有すること

1.1.5 「**顧客**」とは、発注書に記載されている Kantar の関連会社をいいます。

1.1.6 「**顧客データ**」とは、顧客もしくはクライアントによって、または顧客もしくはクライアントに代わって提供される、あるいはサプライヤが本契約に従って生成、処理、保存、または送信することが求められる、データ（顧客またはそのクライアントのスタッフ、顧客／クライアント、サプライヤに関連する個人情報を含む）、文書、テキスト、図面、図、仕様書、画像（およびこれらで構成されるデータベース）をいいます。

1.1.7 「**データ保護法**」とは、GDPR、欧州のプライバシーおよび電子通信に関する指令（その改正を含む）、各国において当該指令を施行する法律をいいます。

1.1.8 「**成果物**」とは、本サービスの一環として提供されるすべての商品、品目、機器および資料をいいます。

1.1.9 「**料金**」とは、発注書に記載されている顧客が支払う合計金額をいいます。

1.1.10 「**GDPR**」とは、個人データ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欧州議会および理事会による 2016 年 4 月 27 日の規則（（EU）2016／679）、および廃止予定の 95／46／EC 指令をいいます（一般データ保護規則）。

1.1.11 「**知的財産権**」とは、すべての特許、発明の権利、著作権および関連する権利、人格権、データベース権、半導体集積回路配置法、実用新案、デザイン権、商標、サービスマーク、商号、ドメイン名、営業権、非公開情報または秘密情報の権利、または現在もしくは将来的に世界各地に存在する可能性のあるその他の類似もしくは同等の権利または保護方法をいいます。

1.1.12 「**個人データ**」は、別紙 3 に定義します。

1.1.13 「**発注書**」とは、本契約条件に添付された発注書、または発注書番号が記載され、本契約条件が適用されるその他の形式の書面によるやり取りをいいます。

1.1.14 「**本サービス**」とは、発注書において指定されるサービス、またはその他の形式の書面によるやり取りにおいて発注書番号を参照して指定されるサービスをいいます。

1.1.15 「**サプライヤ**」とは、発注書において特定される法人をいいます。

1.1.16 「**サプライヤ要員**」とは、本サービスの実施に要する人員をいいます。

1.1.17 「**サプライヤポリシー**」とは、顧客からサプライヤに随時通知されるか、または顧客が運営するエクストラネット（要請に応じて提供）においてサプライヤに提供される、The Kantar Group Limited.およびその直接的または間接的な子会社のサプライヤに適用されるすべてのポリシーまたは行動規範をいい、本契約において別紙 1 として添付されている Kantar ビジネス行動規範および適用可能な Kantar 贈収賄禁止ポリシーなどが含まれます。

2. **サービス**

2.1.1 本契約条件は、本サービスに適用されるものとします。

2.1.2 発注書は、本サービスの開始をもって受理されたものとみなします。サプライヤは、発注書の指定日から本サービスを提供するものとします。サプライヤは、適時、顧客の要望、サプライヤポリシー、業界のベストプラクティス、および本契約の条件に従って、顧客に本サービスを提供するものとします。本サービスを実施する時間は、重要な要素です。

2.1.3 サプライヤは、各サプライヤ要員について以下の内容を保証します。

(a) 随時更新されるサプライヤポリシーを遵守すること。

(b) 本サービスを提供するために適切な資格を有し、訓練を受けていること。

(c) 顧客が発行した特定の指示に従い適切なスクリーニングを受け、刑事上の有罪判決を受けていないこと。

(d) 本サービスが提供されている地域で働く権利を有すること。

2.1.4. サプライヤは、以下の内容を継続的に保証、約束、および表明します。

(a) 本契約に基づく義務を履行する完全な能力および権限を有すること。

(b) 適用される法律、規則、および行動規範にすべて従うこと。

(c) 顧客またはそのクライアントの評判に実質的に悪影響を与える、またはその可能性のある、本契約に基づく義務の履行に関する、いかなる行為または不作為も行わないこと。

(d) 成果物が完全、正確、非侵害で、すべての点において本契約を遵守したものであること。

3. **料金**

3.1 サプライヤは、本サービスの完了時に顧客が合理的に十分であると判断した場合にのみ、顧客に請求できるものとします。

3.2. 顧客は、正確な発注書番号を指定した有効な請求書を受領した月の月末から 60 日後の顧客の次回の支払い処理時に本

サービスの料金を支払うものとします。顧客がクライアントのためにサプライヤから本サービスを受けている場合、顧客は、クライアントから支払いを受けるまでサプライヤに支払いを行う義務を負わないものとします。料金には、売上税またはそれに類する税金は含まれていません。顧客は、法律により求められる場合、料金から控除または源泉徴収を行うことができます。

3.3. サプライヤは、明らかに支払い期限が到来している金額に対して、イングランド銀行の年率ベースレートを 2% 上回る率で利息を請求することができます。

4 契約の解除

4.1 顧客は、以下の場合には、本契約の全部または一部をいつでも解除することができます（一部解除の場合には、それに応じた料金の減額を適用）。

4.1.1 便宜上、サプライヤに対して 30 日前までに書面による通知を行った場合。

4.1.2 サプライヤが本契約の重大な違反を犯し、顧客から是正を求める通知を受けてから 14 日間以内に是正されなかった場合。

4.1.3 サプライヤの解散命令が出されたまたは解散の決議が可決された場合、サプライヤの資産に対して財産保全管理人または更生管財人が任命された場合、裁判所または債権者が財産保全管理人または管財人を任命したり、裁判所が解散命令または管財命令を出したり、債権者との和議を結んだりすることができる状況が生じた場合、または

4.1.4 サプライヤが支払い期限の到来した負債の支払いができなかった場合。

4.2 本契約または本サービスの満了もしくは解除の際に、サプライヤはすべての秘密情報を顧客に引き渡し、顧客および／または第三者と連携して、十分な引き継ぎを保証します。

4.3 本契約の満了または解除によって、終了日までに発生した権利、または契約終了後も明示的もしくは黙示的に存続する条項は損なわれないものとします。

5. 監査

5.1 サプライヤは、本契約の期間中およびその後 6 年間、一般に認められた会計原則および文書保管原則に従って、本サービスに関連する書面による正確な帳簿および記録（タイムシート、クレーム記録、請求書、経費、費用、クレジットノートなど）を主たる事業所に保管および維持するものとし、書面による合理的な通知を受けた場合、顧客および／またはそのクライアント、もしくは顧客の権限を有する代理人が、本契約（第 10 条に定める制限などを含む）の遵守を評価することを目的として当該記録を検査することを許可するものとします。監査の結果、顧客が本サービスに関連する過払い、または本契約の条件の不履行を発見した場合、サプライヤは、自費で当該不履行を是正し、過払い金および関連する監査費用の全額を顧客にただちに返金するものとします。

6. 賠償責任および補償

6.1. 本契約のいかなる規定も、以下のいずれの請求に関する当事者の責任も除外または制限しないものとします。

6.1.1. 当該当事者の過失に起因する死亡または人身傷害に対する請求。

6.1.2. 当該当事者による不正な虚偽の表示を含む不正行為に起因する請求。

6.1.3. 他の方法では合法的に制限または除外することができない責任に対する請求。

6.1.4. 本契約に基づきサプライヤが顧客に提供する補償に対する請求。

6.1.5. サプライヤによる第 8 条から第 10 条までの違反または第 12.1 条の違反に対する請求。

6.1.6. サプライヤによる意図的または故意の不履行に対する請求。

6.2. 第 6.1 条に従って、顧客は、いかなる間接的損失、特別損失、派生的損失または逸失利益（直接または間接を問わず）、営業権の喪失、事業の喪失、収益の損失または予定貯蓄の損失についても責任を負わないものとします。

6.3. サプライヤは、以下のいずれかに起因または関係して顧客が負担したおよび／または被った損失、費用、賠償責任、損害、経費、請求および手続きについて、すべて顧客に補償するものとします。

6.3.1. 本契約の違反。

6.3.2. 本サービスの提供中における顧客の財産に対する損失または損害。

6.3.3. 本契約に関連するサプライヤ、サプライヤ要員および／または下請業者もしくはその従業員による過失行為または不作為。

6.3.4. 成果物および／または本サービスの利用が第三者の知的財産権を侵害しているとの主張。

6.4. 第 6.1 条および第 6.2 条に従って、本契約に起因または関連する顧客の賠償責任総額（過失またはその他を含む契約不履行によるものか不法行為によるものかは問わない）は、当該賠償責任の原因となった事象に先立つ 12 ヵ月間において、本契約に基づいて顧客がサプライヤに支払ったまたは支払うべき料金に等しい金額を超えないものとします。

6.5. 第 6.1 条および第 6.2 条に従って、本契約に起因または関連するサプライヤの賠償責任総額（過失またはその他を含む契約不履行によるものか不法行為によるものかは問わない）は、1 件の請求について 10,000,000 ポンドを超えないものとします。

7. 保険

7.1. サプライヤは、本契約に基づくサプライヤの義務と責任および以下の内容をカバーする定評ある第三者の保険会社の保険に加入し、かつ維持するものとします。

7.1.1. 一般的な賠償責任に関しては、1 件の事象に対して最低 1,000,000 ポンドで、関連する保険期間内は無制限であること。

7.1.2. 雇用者の賠償責任に関しては、1 件の事象に対して最低 5,000,000 ポンドで、関連する保険期間内は無制限であること。

7.1.3. 専門業務に関する賠償責任に関しては、1 件の事象に対して最低 1,000,000 ポンドで、関連する保険期間内は無制限であること。

7.2. 当該各保険契約は、顧客を追加被保険者として指定し、本人に対する補償条項を含むものとします。当該各保険契約は、掛金不要で、顧客が利用できる他の保険の保険金額を超えないものとします。顧客は、払い戻し可能な控除免責金額に関しては責任を負わず、かかる控除免責金額は 50,000 ポンド以上とします。

7.3. サプライヤは、顧客が随時合理的に必要とする追加保険に加入するものとします。

8. データの保護

8.1 本サービスの提供が顧客に代わってサプライヤによる個人データの処理を必要とする場合、サプライヤはデータ保護法の第 7 原則に従うと同時に、以下のとおり対応します。

8.1.1. データ保護法に従います。

8.1.2. データコントローラとして顧客の指示にのみ従います。

8.1.3. 別紙 2（情報セキュリティに関する補遺）に従います。

8.1.4. 別紙 3（データの保護：GDPR）に従います。

8.2. サプライヤは、データ保護法の第 8 条および別紙 3 の規定に従わなかった結果と

して、顧客が被ったまたは顧客が負担したすべての損失、賠償責任、請求、経費、損害、および費用について、顧客に補償するものとします。

8.3. サプライヤは、別紙 3 に定める個人データの処理を必要とする本サービスに関して、GDPR が要求する特定の条件を遵守するものとします。

8.4. サプライヤは、ISO／IEC 27001 情報セキュリティ基準またはそれに随時置き換わる同等の*基*準を組み込んだ措置を講じていることを保証します。

9. **知的財産権**

9.1. 第 9.2 条に従い、顧客は、成果物の知的財産権を所有し、サプライヤは、顧客に対する完全な権限保証を伴い、無条件かつ取消不能な形で、成果物におけるすべての知的財産権をその作成時に譲渡するものとします。サプライヤは、当該成果物に関して絶対的かつ取消不能な形で、顧客に有利となるように人格権（存在する場合）を放棄し、サプライヤ要員に対してこれを放棄させるよう取り計らうものとします。

9.2. 本契約書のいかなる規定も、サプライヤが独自に使用もしくは開発した本サービスの資料、または本サービスの実施に際してサプライヤが使用した（ただし開発はしていない）サプライヤの一般的な方法、ツール、技術またはプロセス（以下「サプライヤの既存資料」と総称する）のサプライヤによる所有権に影響を与えるものではありません。サプライヤの既存資料（もしくはその一部）が成果物に組み込まれている場合、または本サービスを利用または活用する必要がある場合、サプライヤは、顧客が本サービスの完全な利益を得られるようにするために、サプライヤの既存資料を使用するための永続的、全世界共通、取消不能、非独占的、ロイヤリティフリーのライセンスを顧客に付与します。

9.3. サプライヤは、本契約に基づいて付与または譲渡されたすべての知的財産権を譲渡またはライセンスする権利を有すること、およびそれぞれの譲渡またはライセンスがいかなる第三者の知的財産権も侵害してはならないことを保証し、表明します。

9.4. サプライヤは、本契約の理由により、第三者が所有または顧客にライセンスした知的財産権に関する権利、権原または利益を取得しないものとし、サプライヤは、かかるすべての知的財産権が顧客および／またはそのライセンサーの財産であることを認めます。

10. **賄賂の禁止**

10.1. サプライヤは、米国海外腐敗行為防止法（合衆国法典第 15 編セクション 78dd-2、以下「FCPA」という）および英国贈収賄防止法 2010（以下「UKBA」という）を遵守し、そのグループ会社、関連会社ならびにそれぞれの取締役、従業員、代理人および仲介業者、または顧客にサービスを提供している当事者（それぞれを「関係者」という）が FCPA および UKBA を遵守するように取り計らうものとします。

10.2. サプライヤは、その法的義務に違反して、またはその影響力を行使して行為や決定に影響を与えたり（不適切な役割の実施を含む）、顧客のためにビジネスを取得または保持したりするように誘導して、直接的または間接的に、金品などを要求したり、受領に同意したり、受け取ったりしてはならず、各関係者がこのような行為を行うように取り計らってはなりません。サプライヤは、FCPA、UKBA または本第 10 条の違反を認識した場合は、速やかに顧客に書面で通知するものとします。

11. **顧客およびクライアントの資料**

11.1. 本サービスを実施するためにサプライヤに提供された顧客または顧客のクライアントの財産権は、顧客またはそのクライアント（該当する場合）に残るものとします。

11.2. 合理的な事前通知を条件として、顧客またはそのクライアントは、サプライヤか

らいつでもその財産の所有権を取り戻す権利を有するものとします。

11.3. サプライヤは、顧客または顧客のクライアントが所有する財産を安全に保持するものとし、本サービスの実施に必要な場合を除き、書面による顧客またはそのクライアントの同意を得ずに、当該財産の処分または当該財産の所有を放棄してはなりません。

11.4. サプライヤは、顧客または顧客のクライアントの財産に関するリーエンまたはその他の権利を放棄し、かかる財産にすべてのリーエンおよびその他の負担がかからないようにするものとします。

11.5. サプライヤは、顧客または顧客のクライアントが関係するサービスの実施に関連して、顧客または顧客のクライアントの財産のみを使用するものとします。

12. **現代奴隷法**

12.1. サプライヤは、サプライヤ、その役員、従業員、代理人または下請業者のいずれもが以下に該当しないことを保証します。

12.1.1. 2015 年度現代奴隷法に基づく違反行為（以下「MSA 違反」という）を行った。

12.1.2. 2015 年度現代奴隷法に基づく MSA 違反の疑いまたは訴追に関する調査の対象であるとの通知を受けた。

12.1.3. サプライチェーン内において、2015 年度現代奴隷法に基づく MSA 違反の疑いまたは訴追に関する調査の原因となる何らかの状況があることを認識している。

12.1.4. 2015 年度現代奴隷法を遵守すること。

12.1.5. サプライヤ、その役員、従業員、代理人または下請業者が本第 12 条に基づくサプライヤの義務に違反している、またはその可能性があると認識した場合、またはそのように考えるべき理由がある場合には、ただちに書面で顧客に通知すること。

13. **一般**

13.1. サプライヤは、本契約期間中およびその後 5 年間、すべての秘密情報の守秘義務を遵守し、本サービスを実施するために厳密に必要な場合または法律で要求される場合を除き、当該秘密情報の使用または第三者への開示を行わないものとします。

13.2. いずれの当事者も、顧客が The Kantar Group Ltd.の（直接的または間接的な）子会社に権利を譲渡することができる場合を除き、書面による他方当事者の事前同意を得ずに、本契約に基づく権利または義務を譲渡、委託、またはその他の方法によって譲渡することはできません。

13.3. 本契約の各条項は、分離可能であり、他の条項から区別されます。特定の条項が無効または執行不能である場合であっても、本契約の他の条項には影響を与えないものとします。

13.4. 本契約に定められている権利もしくは救済、またはコモンロー上もしくはエクイティ上の権利もしくは救済の不履行または遅延が生じた場合であっても、当該権利もしくは救済、またはその他の権利もしくは救済を放棄したことにはならないものとします。

13.5. 本契約のいかなる規定も、両当事者間のパートナーシップまたは代理関係を確立するまたは暗示するとは解釈されないものとします。

13.6. 本契約は、本契約内で取り扱われる事項に関する両当事者間の完全な合意および理解を構成するものであり、当該事項に関する両当事者間のいかなる以前の合意にも優先します。本契約は、書面による顧客およびサプライヤの同意のみに基づき改訂することができます。

13.7. 本契約の当事者以外の者は、1999 年契約（第三者の権利）法に基づくいかなる権利も有しません。

13.8. 本契約に基づいて行うべきいかなる通知も、書面によるものとし、発注書の記載住所宛てに第一種郵便または特別配達郵便にて送付され、他方当事者に手渡しされた場合にのみ、有効とします。

13.9. 本契約および非契約上の義務には英国法が適用されるものとし、両当事者は、いかなる紛争も英国の裁判所の非専属管轄権に付託することに合意します。

別紙 1 : KANTAR ビジネス行動規範

Kantar およびそのグループ企業は、世界中の多くの市場または国において事業を展開しています。いかなる場合も、当グループは、英国の贈収賄法や米国の海外腐敗行為防止法および 2015 年度現代奴隷法（関連する場合）および業界の行動規範などの国内法およびその他の国際的な法律を尊重します。当グループは、ビジネスのすべての側面において倫理的に行動すること、および最高水準の実直さと誠実さを維持することに取り組んでいます。

当グループは、サプライヤを含むすべてのビジネスパートナーが同様に倫理的行動に取り組むことを期待し、これを求めています。したがって、当グループのビジネス行動規範（下記表の第 1 列）への同意について確認を求めます。Kantar グループ以外の企業の場合には、必要に応じて下記表の第 2 列の内容に基づく修正が適用されます。

当グループは、すべてのサプライヤがこれらの基準および適用される国際法の遵守を促進および監視する適切なシステムを使用することを期待しています。

当グループは、サプライヤが本規範の原則に対する取り組みを示すこと、およびサプライヤの業務に関連する環境、労働安全衛生および倫理リスクを特定するためのリスク管理プロセスを実行していることを期待しています。

サプライヤは、スタッフが脅迫や報復を受けることを恐れることなく、懸念を報告するように促す必要があります。サプライヤは、必要に応じて適切な措置を講じなければなりません。

サプライヤは、自らのサプライチェーンに対して、本規範と同等の基準を設ける必要があります。

Kantar の行動規範	**Kantar がサプライヤに期待すること**
Kantar グループ（以下「当グループ」という）内における全企業の役員およびスタッフは、株主、クライアント、スタッフ、サプライヤを含む当グループの業績に利害関係を有するすべての者に対する義務を認識しています。	当グループの義務を認識し、これらの義務に悪影響を与えないことを確認します。
当グループの事業に関する情報は、現地の規制に従って、差別のない方法で明確かつ正確に伝達されるものとします。	Kantar グループに関する情報を定められているとおりに取り扱うことを確認します。
当グループは、人種、宗教、国籍、肌の色、性別、性的指向、性同一性もしくは性表現、年齢または障害に対する差別や懸念なく、資質および実力に基づく人事を行っています。	所属する組織内に同等のポリシーが設けられていることを確認します。

当グループは、職場が安全で互いを尊重し合うべき場であり、職業は自由に選択されるべきものであると考えており、性的嫌がらせ、言葉や行為による個人に対する執拗な侮辱を含む差別やあらゆる種類の侮辱的な行為、侮辱的な内容の表示や配布、Kantar またはクライアントの施設における武器の使用や所持を容認しません。	所属する組織内およびサプライチェーンに同等のポリシーが設けられていること、また当グループの職場および従業員を定められているとおりに尊重することを確認します。 具体的には以下の通りです。 • 職業は自由に選択されるべきものであり、強制労働またはその他の現代の奴隷に相当する労働を使用してはなりません。 • 雇用の条件として、労働者にパスポートや政府発行の身分証明書の提出を強制してはなりません。 • 児童労働を使用してはなりません。 • 労働者に対する報酬は、すべての適用される賃金法に準拠していなければなりません。 • 1週間の労働時間は、現地法で定められた上限を超えてはなりません。 • 性的嫌がらせ、性的虐待、体罰、身体的強制、言葉による侮辱を含む非人道的な待遇があってはなりません。 • Kantar はサプライヤに対し、すべての労働者にとって安全な労働環境を作り、育成することを期待します。 • 可能な限り、労働者に対する物理的危険を除去し、それが不可能な場合には管理する必要があります。 • サプライヤは、労働者に影響する緊急事態に対応するための適切な手順を設ける必要があります。 • 業務上の傷害および病気を管理、追跡、報告するシステムが設けられている必要があります。
当グループは、違法薬物の使用、所持、配布、または薬物やアルコールの影響を受けた状態で出勤している従業員を容認しません。	所属する組織内に同等のポリシーが設けられていること、また当グループの職場および従業員を定められているとおりに尊重することを確認します。

当グループは、当グループの事業またはクライアントに関連するすべての情報の守秘義務を遵守します。特に、「インサイダー取引」は、明示的に禁止されており、秘密情報を個人的な利益のために使用してはなりません。	当グループの情報に関するポリシーに同意していることを確認します。
当グループは、国内法および業界規範に従って、消費者、クライアントおよび従業員のデータ保護に取り組んでいます。	所属する組織内に、当グループの事業および当該事業における当グループのパートナーの事業に関するすべての情報を対象とする同等の取り組みが設けられていることを確認します。
当グループは、一般公衆の礼儀に反する声明、提案または画像を含む業務を意図的に行うことはなく、人種、宗教、国籍、肌の色、性別、性的指向、性同一性または性表現、年齢または障害などによる少数派に対する影響を適切に考慮します。	必要に応じて所属する組織の業務に対して同様の基準が設けられていることを確認します。
当グループは、社会、環境、人権に関する問題を含め、誤解を招くような意図や目的をもった業務を引き受けません。	必要に応じて所属する組織の業務に対して同様の基準が設けられていることを確認します。
当グループは、クライアントまたは業務が当グループの評判を損なう可能性について考慮したうえで、これを引き受けます。これには、人権侵害をもたらす活動に関与しているクライアントとの関係による風評被害が含まれます。	これは、Kantar グループのメンバーにのみ関係します。
当グループは、個人または家族の利益のために、グループ内の企業または当該企業に対する当グループの義務と競合する活動に直接的にも間接的にも関与しません。	これは、Kantar グループのメンバーにのみ関係します。
当グループは、現金かどうかを問わず、公務員、クライアント、ブローカーまたはこれらの代理人などを含む第三者との間において贈収賄または贈収賄の申し入れを行いません。当グループは、トレーニング、コミュニケーション、および例を示すことにより、すべての従業員が本ポリシーを理解していることを共同で確認します。	これは、そのまま適用されます。
当グループは、個人的な利益のために、サプライヤ、潜在的なサプライヤまたは他の第三者から名目上の価値を上回る商品またはサービスを受け入れません。	これは、そのまま適用されます。

当グループは、当グループ内、または当グループのサプライヤもしくは当グループと取引のある第三者との間において、個人的または家族的な利益相反に当たる行為を行いません。	所属する組織内に同等のポリシーが設けられている必要があります。
書面による Kantar 取締役会の事前承認を得ることなく、政治家、政党または活動委員会に対する市場価値を下回る価格でのサービスや商品の提供を含むいかなる種類の企業献金も行うことはできません。	適切な承認手続きとともに、このような献金に関する独自のポリシーを設けている必要があります。
当グループは、高いマーケティング倫理基準の維持、当グループの事業、サプライチェーン、およびクライアントの業務における人権の尊重、環境の重視、地域組織の支援、従業員による開発の支援、サプライチェーンにおける重要な持続可能性リスクの管理によって、社会と環境に対する積極的な貢献を行う努力を継続します。当グループの持続可能性に関するポリシーおよび人権に関するポリシーには、これらの分野における当グループの取り組みに関するより詳細な内容が定められています。	所属する組織内に同等のポリシーが設けられている必要があります。具体的には以下の通りです。 • サプライヤは、英国の現代奴隷法を遵守する必要があります。 • サプライヤは、廃棄物および排出物を含むすべての関連する環境認可を取得する必要があります。 サプライヤは、材料の再生、再利用、代替による施設やプロセスの保全措置を実施して汚染防止に努めなければなりません。

当社は、当社のために改訂された Kantar のビジネス行動規範を遵守することを確認します。当社は、特に賄賂または不適切な贈答品、または貴社またはその他の第三者との間でのサービスに関連し、または、直接またはその関連によって Kantar の評判を損なう可能性のあるその他の事項に関する違反を認識した場合、直ちに貴社に通知します。

署名：

記名：

役職：

組織名：

日付：

別紙 2 : 情報セキュリティに関する補遺

1 はじめに

本セキュリティ要件に関する別紙（以下「本別紙」という）は、顧客および顧客のクライアントの秘密情報の秘密保持、可用性および完全性を確保するために必要なサプライヤの情報セキュリティに関する基本要件を定めています。サプライヤは、本契約に基づくサプライヤによるサービスの実施を通じて、これらの要件を遵守するものとします。

2. 用語

2.1. 本別紙で使用する場合、以下の各用語を次のとおりに定義します。本契約においてその他の未定義語が用いられた場合、本契約において各用語に付与された意味を有するものとします。

2.2. 「**請負業者**」とは、顧客および顧客のクライアントの秘密情報の保存、処理、取扱いを行う、または当該情報にアクセスするサプライヤの下請業者、独立契約者、サービスプロバイダまたは代理人をいいます。

2.3. 「**慎重な取り扱いを要する顧客の情報**」とは、個人データ［電子メール、氏名など］、健康情報、財務情報または投資に関する保有情報を含む顧客および顧客のクライアントの秘密情報をいいます。

2.4. 「**暗号化**」とは、情報の秘密性、完全性、および／または真実性を保護するためのメカニズムとして、元の形式（平文）から難読化された形式（暗号文）への可逆的なデータの変換をいいます。暗号化には、暗号化アルゴリズムおよび 1 つまたは複数の暗号鍵が必要です。

2.5. 「**保存**」とは、保存、アーカイブ、バックアップおよび／またはこれらに類似する行為を実行することをいいます。

3. セキュリティレビュー

3.1. サプライヤは、顧客および顧客のクライアントの秘密情報を処理、保存、または他の方法によるアクセスを行う期間全体にわたって、サプライヤのセキュリティプログラムを毎年オンサイトでレビューする権利を顧客に提供するものとします。サプライヤは、相互に同意可能な日を決定するために当該レビューを速やかに（いかなる場合においても、顧客による当該レビューの計画および実施の要請を受けてから 30 日を超えずに）計画します。

3.2. サプライヤは、サプライヤのポリシー、手順およびその他の関連文書、ならびに当該レビューの促進に合理的に必要なサプライヤ要員に顧客がアクセスする権限を与えるものとします。サプライヤは、当該レビューの完了後 30 日以内に顧客に是正措置計画を提出し、両当事者が合意した是正措置計画に従って、適時に各問題を是正するものとします。

4. 特定のセキュリティ要件

4.1. セキュリティポリシー

サプライヤは、少なくとも以下の内容を含む書面による包括的なセキュリティポリシーおよび手順を維持するものとします。

4.1.1. サプライヤによる情報セキュリティへの取り組み。

4.1.2. 情報の分類、表示、取扱い、情報の取扱いに関するポリシーおよび手順には、情報の伝達、保管、廃棄のために許容される方法を定め、このような方法は、以下に定める顧客

によるサプライヤ情報の保護に関するガイドラインに定める方法を上回る保護基準を備えたものであること。

4.1.3. コンピューティングシステム、ネットワーク、およびメッセージングを含むサプライヤの資産の使用許可。

4.1.4. データ侵害に関する通知およびエビデンス収集に関する手順を含む情報セキュリティインシデント管理。

4.1.5. エンドユーザー、管理者、およびシステムのパスワードの形式、内容および使用法に関する認証規則。

4.1.6. アクセス権限の定期的なレビューを含むアクセス制御。

4.1.7. 当該ポリシーおよび手順を遵守していない要員に対する懲戒処分。

4.1.8. 本第 4 条に定められているトピックの適用可能な要件と矛盾しない形で本第 4 条の残りの部分に定められているトピック。

サプライヤは、そのポリシーに重大な変更があった場合、30 日以内に Kantar に通知するものとします。

4.2. **サプライヤの情報セキュリティプログラムに関する責任**

サプライヤは、サプライヤの情報セキュリティプログラムを維持し、情報セキュリティおよび情報リスク管理を実施するように指定されたスタッフと共に、情報セキュリティに関する責任を負うものとします。

4.3. **サプライヤの情報セキュリティプログラムの監査、レビューおよびモニタリング**

サプライヤは、顧客および顧客のクライアントの秘密情報に対するリスクを制限するための保護措置が適切なものであることを保証するために、サプライヤの情報セキュリティプログラムを定期的に監視およびレビューするものとします。

4.4. **資産および情報管理**

サプライヤは、以下のとおり対応するものとします。

4.4.1. サプライヤが処理または保存する顧客および顧客のクライアントのすべての秘密情報の一覧を維持すること。

4.4.2. サプライヤが本契約に基づく活動を実施する際に使用する物理的なコンピューティング資産およびソフトウェア資産の一覧を維持すること。

4.4.3. 顧客および顧客のクライアントの秘密情報の取扱い、処理、および保存の際に、以下に定める顧客によるサプライヤ情報の保護に関するガイドラインに従うこと。

4.5. **物理的および環境的なセキュリティ**

サプライヤは、以下のとおり対応するものとします。

4.5.1. 顧客および顧客のクライアントの秘密情報を保存、アクセス、または処理するサプライヤの領域への立ち入りを当該アクセスの許可を得たサプライヤ要員のみに制限すること。

4.5.2. 消防、冷却、電力、緊急システム、および従業員の安全を含むインフラシステムに対する合理的なベストプラクティスを実施すること。

4.5.3. 顧客および顧客のクライアントの秘密情報を保存、アクセス、または処理するすべての領域に対する、顧客および顧客のクライアントの秘密情報の秘密性に見合った物理的な立ち入り制限を行うこと。

4.5.4. 顧客および顧客のクライアントの秘密情報の取り扱い、保存、および／または処理をする領域を定期的に監視すること。

4.6. **従業員に関連する問題**

サプライヤは、以下のとおり対応するものとします。

4.6.1. 適用法により制限または禁止されている場合を除き、各サプライヤ要員（法律で許可されている場合、顧客および顧客のクライアントの秘密情報にアクセスできる請負業者も含む）の犯罪歴チェックを実行すること。当該犯罪歴チェックは、当該個人が顧客および顧客のクライアントの秘密情報にアクセスすることを許可される前に実施すること。サプライヤは、十分な犯罪歴チェックを受けていない個人が顧客および顧客のクライアントの秘密情報にアクセスすることを許可しないこと。

4.6.2. サプライヤの秘密情報およびサプライヤに委託された他の企業の秘密情報（顧客および顧客のクライアントの秘密情報など）の好ましい使用法および取扱いに関して、新規要員（請負業者を含む）に対する訓練を実施すること。

4.6.3. サプライヤ要員（請負業者を含む）に対するセキュリティおよびデータプライバシーに関する教育および訓練を実施し、当該教育を修了した要員の記録を維持すること。

4.6.4. サプライヤの情報システムおよびサービスへのアクセスを許可および取り消すための正式なユーザー登録および登録解除の手順を実施すること。サプライヤ要員（請負業者を含む）の退職時に、サプライヤは、当該個人による顧客および顧客のクライアントの秘密情報へのアクセス権限をできる限り早く取り消すものとすること（いかなる場合も、当該個人の退職後 2 営業日を超えないこと）。

4.7. **通信および操作**

サプライヤは、以下のとおり対応するものとします。

4.7.1. 合意された復旧期間内に（または、両当事者によって特定の復旧期間が合意されていない場合には、商業的に合理的な期間内に）顧客に対するサービスを復旧するために十分な定期バックアップを実行すること。

4.7.2. 以下に定める顧客によるサプライヤ情報の保護に関するガイドラインに従い、顧客および顧客のクライアントの秘密情報が含まれるすべてのバックアップメディアを暗号化すること。

4.7.3. 書面による顧客の事前同意を得ずに、顧客および顧客のクライアントの秘密情報をサプライヤの施設外で保存または複製しないこと。

4.7.4. 書面による顧客の事前同意を得ずに、顧客および顧客のクライアントの秘密情報を第三者に送信、移転または提供したり、第三者に顧客および顧客のクライアントの秘密情報へのアクセス権限を提供したりしないこと。

4.7.5. 前第 4.7.3 条および 4.7.4 条に定められている行為を顧客が承認している場合、顧客および顧客のクライアントの秘密情報を保存または複製する第三者および／またはサプライヤの施設外の場所、顧客および顧客のクライアントの秘密情報を受け取るまたは当該情報へのアクセス権限を受け取る第三者、当該顧客および顧客のクライアントの秘密情報を保存、複製、提供または当該情報へのアクセス権限を保存、複製、提供する目的、当

該第三者に対する当該顧客および顧客のクライアントの秘密情報の送信またはその他の手段による提供方法、当該顧客および顧客のクライアントの秘密情報の送信またはその他の手段による提供の際に使用した送信および暗号化／保護方法またはプロトコル（該当する場合）、第三者に対して送信またはその他の手段により提供された顧客および顧客のクライアントの秘密情報の詳細、当該手配を承認した顧客の従業員の氏名および当該承認を得た日付を含む一覧を維持すること。

4.7.6. 顧客および顧客のクライアントの秘密情報を消去または破棄する場合、安全なデータの無害化に関する米国防総省基準（DOD 5220.22M）を満たすデータ破棄手順を採用すること。サプライヤは、顧客の書面による要請に応じて、すべての顧客および顧客のクライアントの秘密情報を速やかに消去または破棄すること。

4.7.7. 顧客および顧客のクライアントの秘密情報を送信または移送する際の暗号化に関するガイドラインを含む、以下に定める顧客によるサプライヤ情報の保護に関するガイドラインに従うこと。

4.7.8. 顧客および顧客のクライアントの秘密情報が保存されている、または顧客および顧客のクライアントの秘密情報にアクセスするサプライヤ要員が使用するすべてのノート PC に対してハードディスクの暗号化を使用し、当該暗号化は、以下に定める顧客によるサプライヤ情報の保護に関するガイドラインに従うこと。

4.7.9. 顧客および顧客のクライアントの秘密情報を送信、アクセス、処理または保存するサプライヤのサーバーおよび／またはエンドユーザーのプラットフォーム上において、最新のマルウェア検出および防止対策を維持すること。

4.7.10. ファイアウォール、ウイルス対策、マルウェア対策、侵入検知システム、および商業的に妥当なその他の保護技術を使用して、強固なインターネットとの境界を維持し、インフラを保護すること。

4.7.11. 顧客および顧客のクライアントの秘密情報を送信、アクセス、処理または保存するサプライヤのすべてのシステムに対して、定期的なパッチ管理およびシステム保守を実施すること。

4.8. **アクセス制御**

サプライヤは、以下のとおり対応するものとします。

4.8.1. ユーザー認証に対するベストプラクティスを実施すること。顧客および顧客のクライアントの秘密情報にアクセスする個人または自動化プロセスの認証にパスワードを使用する場合、当該パスワードは、パスワードの使用、作製、保存、および保護に関する現行のベストプラクティスに準拠すること。（下記の顧客によるサプライヤ情報の保護に関するガイドラインを参照）。

4.8.2. ユーザー ID が個人に対する一意なものであり、共有されていないこと、およびサプライヤのユーザーの終了から 48 時間以内に削除することを確認すること。

4.8.3. 顧客および顧客のクライアントの秘密情報の秘密性、個人の業務に関する要件、および特定の顧客および顧客のクライアントの秘密情報に対する個人の「知る必要性」に基づきアクセス権限を割り当てること。

4.8.4. 「知る必要性」に基づく制限を確実に最新の状態に保つために、サプライヤ要員（請負業者を含む）のアクセス権限を少なくとも年 1 回レビューすること。

4.8.5. ユーザーによる顧客および顧客のクライアントの秘密情報を保管しているサプライヤの施設への立ち入りに関するレポートを定期的にレビューすること。

4.8.6. 顧客および顧客のクライアントの秘密情報を机やプリンタの上、またはサプライヤの施設内のその他の場所に安全が確保されていない状態で放置しないこと。

4.9. **アプリケーション開発、脆弱性スキャンおよび侵入テスト**

サプライヤは、以下のとおり対応するものとします。

4.9.1. 開発ライフサイクル全体にわたってセキュリティを組み込んだ安全な開発方法を実装すること。

4.9.2. 安全なコーディング基準を開発し、実施すること。

4.9.3. サプライヤ（または請負業者）によって開発され、顧客に提供されたすべての社外向けアプリケーションおよびソフトウェアの自動スキャンツールを使用した安全なコードレビューを実行すること。

4.9.4. 顧客および顧客のクライアントの秘密情報を受信、アクセス、処理または保存するすべての社外向けアプリケーションに対して、少なくとも四半期毎に脆弱性スキャンを実行し、顧客の要請に応じて、サプライヤは、当該脆弱性スキャンを正常に実行したことを書面で確認すること。

4.9.5. 外部の第三者のセキュリティテスト会社を使用し、慎重な取り扱いを要する顧客の情報を受信、アクセス、処理または保存するすべての社外向けアプリケーションに対して、少なくとも年に 1 回侵入テストを実施すること。当該侵入テストは、顧客が承認したサプライヤのテストベンダーによって実施し、顧客の要請に応じて、サプライヤは、当該侵入テストを正常に実行したことを書面で確認すること。また、サプライヤは、サプライヤ自身によってまたはサプライヤに代わって実施された当該侵入テストの過程で発見されたすべての重大な問題を 30 日以内、または当該問題が 30 日以内に是正できない場合には、サプライヤと顧客との間において相互に同意された期間内に是正すること。

4.10. **請負業者**

サプライヤは、以下のとおり対応するものとします。

4.10.1. 適用される法律および規制、ならびに本別紙を含む本契約に定められている要件を上回る保護基準に従って、顧客および顧客のクライアントの秘密情報を保護するためのセキュリティ対策を維持することができる請負業者を選択および維持する合理的な措置を講じること。また、契約によって、当該請負業者に当該セキュリティ対策の実施および維持を要求する書面による契約を当該請負業者と締結すること。

4.10.2. 書面による顧客の事前同意を得ずに、顧客および顧客のクライアントの秘密情報を請負業者に提供しない、または当該情報にアクセスすること、もしくは当該情報を処理、保存、表示またはその他の方法でやり取りすることを請負業者に許可しないこと。

4.10.3. 請負業者が本別紙を含む本契約の条項を遵守しないことを含む、請負業者によるすべての行為および不作為について顧客に対する責任を負うこと。

4.10.4. 請負業者の情報セキュリティポリシーおよび慣行のレビューを含む、各請負業者のレビューを定期的に実施すること。

5. **情報セキュリティインシデント管理**

5.1. サプライヤは、以下のとおり対応するものとします。

5.1.1. 情報セキュリティインシデントへの対応プロセス（特に、エビデンスの保全プロセス、法執行機関、政府機関および必要に応じて同様の当事者への通知およびこれらの機関との連携、ならびにフォレンジック分析の実施を含む）を確立、テスト、および維持すること。

5.1.2. 顧客および顧客のクライアントの秘密情報に関わるセキュリティ違反（顧客および顧客のクライアントの秘密情報への実際の不正アクセスまたはその疑いを含む）、または請負業者のシステム、ハードウェア、機器、装置または施設内コンピュータにおけるまたはこれらに関わる、もしくはその他の方法で請負業者の要員に関わるセキュリティインシデントについて書面で顧客に通知すること。サプライヤは、速やかに、ただしいかなる場合においてもサプライヤが最初に当該インシデントを認識した日から 24 時間以内に、当該インシデントについて通知すること。その後、サプライヤは、当該インシデントの調査および軽減に関して、顧客に定期的な最新情報を提供すること。サプライヤは、顧客またはその被指名人が調査のあらゆる側面に参加することを許可すること。サプライヤは、影響を受けるデータ主体への通知、フォレンジック分析、データ主体に対する信用モニタリング、およびその他是正に関する努力ならびに法的努力などを含む、当該インシデントに関連する当事者が被るすべての費用について責任を負うこと。

5.1.3. 当該各インシデントについて、サプライヤが当該インシデントを終息させてから 10 日以内に、当該インシデントの根本原因、講じられた措置、および今後同様の事象発生を防止する計画に関する詳細な情報を含む最終的な書面による通知を顧客に提出すること。

6. 事業継続性管理

6.1. サプライヤは、以下のとおり対応するものとします。

6.1.1. 想定外の事象が発生した場合に、技術および事業の両方の復旧を対象とする包括的な事業継続計画（以下「BCP」という）を確立し、維持すること。

6.1.2. サプライヤの単独かつ絶対的裁量により、適切であると判断する方法で、少なくとも年に 1 回は BCP をテストまたはレビューすること。

7. コンプライアンス

7.1. サプライヤは、以下のとおり対応するものとします。

7.1.1. 以下に定める顧客によるサプライヤ情報の保護に関するガイドラインに従うこと。

7.1.2. 顧客および顧客のクライアントの秘密情報、ならびに本契約に基づくサプライヤの活動の過程において生成されたまたは当該活動にその他の形で関連して生成された他の情報に適用される記録保持およびデータ破棄のための相互に同意されたポリシーおよび慣行を確立し、維持すること。

7.1.3. 倫理規範を確立し、従業員が毎年それをレビューし、承認するように求めること（法律で禁止されている場合および法律で禁止されている範囲を除く）。

8. フォローアップリスク管理行動

8.1.サプライヤおよび／または 1 箇所もしくは複数のサプライヤの施設（もしくは、該当する場合、請負業者の施設）について、顧客が以前セキュリティレビューを実施したことがある場合、およびかかるセキュリティレビューの結果、懸念事項が顧客によって特定された場合、サプライヤは、

8.1.1. まだ顧客との協力ができていない場合には、顧客と合理的に協力して、当該懸念事項を是正するための相互に同意可能なリスク管理計画を迅速に作成し、

8.1.2. 当該リスク管理計画に定められている対策を当該リスク管理計画に定められている日までに実施するものとします。

8.2. 最新のセキュリティレビューのためのリスク管理計画は以下に規定されています。または、以下の表が空白の場合は、当事者によって作成され、合意された別の文書に記載されるものとします。

リスク管理計画		
重要度	行動計画	日付
高		
中		
低		

9. **個人情報の盗難**

サプライヤが個人情報を処理、取扱い、またはアクセスする場合において、本契約に基づくサプライヤの活動の過程で、サプライヤの従業員が当該個人情報に関わる個人に関する個人情報の盗難の可能性を認識したときには、サプライヤは速やかに顧客に通知するものとします。

10. **更新**

顧客は、30 日前までにサプライヤに書面で通知することにより、本情報セキュリティに関する補遺を更新することができます。サプライヤが当該更新を遵守できないと判断した場合、サプライヤは、満たすことができない項目を具体的に記載した書面により、当該 30 日間以内に顧客に通知するものとします。このような場合、顧客は、サービスまたはサプライヤとのプロジェクトの全部または一部を終了する権利を留保し、当該終了を理由とする責任または罰則を負わないものとします。

付属文書 1

顧客によるサプライヤ情報の保護に関するガイドライン

顧客による情報分類および取扱いに関するマトリクス

慎重な取り扱いを要する顧客の情報を含む、顧客および顧客のクライアントの秘密情報の送信（もしくは移送）、保存または破棄をする際に適用可能な特定の要件がまとめられています。

情報分類	例	送信	保存	破棄
慎重な取り扱いを要する顧客の情報を含まない顧客および顧客のクライアントの秘密情報	ビジネス戦略と計画、監査報告、リリース前のマーケティング情報、顧客独自のソフトウェア、技術仕様書またはアーキテクチャ	電子媒体の場合：パブリックネットワークを介して送信する場合、または携帯用媒体や携帯用デバイスもしくは他の電子媒体でサプライヤの施設外に移送する場合には、暗号化が必要。 印刷物の場合：宅配便（翌日配達サービスを含む）または追跡番号付きの書留郵便で送付。	許可を受けた要員にのみアクセスを制限。四半期ごとのアクセス権限レビューを実行。保存時には暗号化を推奨。	電子媒体の場合： DOD 5220.22M またはこれに相当する手順を使用。 印刷物の場合：シュレッド
慎重な取り扱いを要する顧客の情報	個人情報（氏名、電子メール、電話番号、郵送先住所、社会保障番号、または口座番号を含む） 個人の財務情報 個人の健康情報	同上	許可を受けた要員にのみアクセスを制限。四半期ごとのアクセス権限レビューを実行。 保存時には暗号化が必須。	同上

暗号化

以下に、顧客が現在推奨している暗号化アルゴリズムおよび現在追加で許容できる暗号化アルゴリズムを示します。サプライヤは、顧客および顧客のクライアントの秘密情報を暗号化する際に、推奨アルゴリズムのうちの 1 つを使用するものとします。ただし、合理的に実現不可能な場合はこの限り

ではなく、この場合には、サプライヤは、顧客および顧客のクライアントの秘密情報を暗号化する際に、追加で許容できる暗号化アルゴリズムのうちの 1 つを使用するものとします。

推奨暗号化アルゴリズム		
目的	**アルゴリズム**	**最短鍵長（ビット）**
鍵の交換	RSA Diffie-Hellman	2048 を推奨（不可能な場合は、1024）
データの保護	CBC モードの AES CBC EDE3 モードの 3DES	256 を推奨（不可能な場合は、128） 168
Hash	SHA-256	該当なし
HMAC	HMAC SHA-256	256
デジタル署名	RSA with SHA-256 DSA with SHA-256	2048 を推奨（不可能な場合は、1024）

追加で許容できる暗号化アルゴリズム		
目的	**アルゴリズム**	**最短鍵長（ビット）**
データの保護	CTR モードの AES RC4 CBC モードの RC5 CBC モードの Blowfish CBC モードの CAST-128 CBC モードの IDEA	2048 を推奨（不可能な場合は、128）
Hash	SHA-2 を推奨（不可能な場合は SHA-1） 技術的に例外が要求されない限り、絶対に MD5 を使用しないこと	該当なし
HMAC	HMAC SHA-2 を推奨（不可能な場合は SHA-1） 技術的に例外が要求されない限り、絶対に	160 128

	MD5 を使用しないこと	
デジタル署名	ECC with SHA-256、SHA-2 RSA with SHA-2 を推奨（不可能な場合は SHA-1） DSA with SHA-2 を推奨（不可能な場合は SHA-1）	160 分 2048 を推奨（不可能な場合は 1024）

パスワードベースの認証ガイドライン

サプライヤ（もしくは請負業者）が管理または制御するすべてのパスワードは、次のガイドラインを満たすものとします。

領域	ガイドライン
最短パスワード長	8 文字
パスワードの複雑さ	個人やプロセスに容易に関連付けらず、辞書には含まれない、パターンを表さない 4 種類の文字種（大文字、小文字、数字、特殊）のうち 2 種類を使用。パスワードには、4 種類の文字種のうちの 3 種類を含むことを強く推奨。
パスワードの最長有効期間	最大 90 日間
最短パスワード履歴	1 日間
送信中の保護	必須。パスワードは送信中に暗号化する必要があります。
ストレージの保護	必須。パスワードは、承認済みのハッシュアルゴリズム（上記表を参照）を使用してハッシュする必要があります。

KANTAR

別紙 3

データの保護

1 **定義**

1.1 本別紙 3 において、本契約で使用されていて他に定義されていない用語は、GDPR に定められている用語定義に従うものとします。

1.1.1 **範囲内の個人データ**とは、本契約に基づく本サービスの提供またはその他の義務の履行の過程でサプライヤが処理する個人データをいいます。

1.1.2 **データ保護**とは、範囲内の個人データの完全性および安全性に対する脅威または危険、当該データの不正なまたは偶発的な破壊、紛失、変更、使用、当該データの不正アクセスから保護し、業界のベストプラクティスに従う管理上、技術的および物理的な保護措置をいいます。

1.1.3 **モデル条項**とは、第三国に設立されたプロセッサーへの個人データの移転に対する標準契約条項に関する 2010 年 2 月 5 日の欧州委員会の決定（2010／87／EU）によって承認された標準契約条項（ただし、欧州委員会がその決定において任意であると指定した契約条項は除外する）で、欧州委員会によって随時改訂または置き換えられる条項をいいます。

1.1.4 **「サブプロセッサー」**とは、本契約との関連において、顧客に代わり範囲内の個人データを処理するようサプライヤによって指名された第三者をいいます。

1.1.5 **「コントローラ」、「データ主体」、「加盟国」、「個人データ」、「処理」、「プロセッサー」**および**「監督当局」**の各用語は、GDPR で使用されるものと同じ意味を持ち、その同根語はそのように解釈されるものとします。任意の国または地域からのデータの移転に対する参照には、その国または地域の外からそのデータにリモートアクセスすることなどが含まれます。

1.1.6 本契約の 2.1.4 条における適用法への参照は、その処理に欧州連合または加盟国の法律が適用される範囲内の個人データに関連して当該条項が適用される範囲において、サプライヤに適用される欧州連合または加盟国の法律に限定されるものとします。

2. 義務

2.1. サプライヤおよび顧客は、本契約に関連するすべてのデータ保護法およびすべての適用されるサプライヤのポリシーに基づき、常にその義務を遵守するものとします。

2.2. サプライヤは、本サービスの提供および本契約に基づくその他の義務の履行以外の目的で、範囲内の個人データを使用またはその他の方法で処理できないものとします。

2.3. 当事者の役割。各当事者は、範囲内の個人データの処理に関し、顧客がコントローラであり、サプライヤがプロセッサーであり、以下の 2.8.4 条に規定された要件を満たす目的のみでサブプロセッサーを関与させることを認め、合意します。

2.4. サプライヤは、以下のとおり対応するものとします。

2.4.1. 書面による顧客の指示に従ってのみ、範囲内の個人データを処理すること。

2.4.2. 範囲内の個人データの誤りまたは不正確性を認識した場合には速やかに顧客に通知すること。

2.4.3. 別段の書面による顧客の指示またはデータ保護法による要求がある場合を除き、サプライヤ、サブプロセッサーまたはサプライヤ要員の所有または管理下にある範囲内の個人データのコピーは、本契約に基づくサプライヤの義務の履行に必要とされなくなった場合、永久に破棄するように努めること。

2.4.4. 範囲内の個人データにアクセスできるのは、次のサプライヤ要員のみであることを徹底すること。（i）本契約に基づくサプライヤの義務の履行においてその役割を果たすためにデータにアクセスする必要がある者、（ii）データの処理、管理および取扱いに適用されるデータ保護法の要件について適切な訓練を受けている者、（iii）範囲内の個人データに関する契約上または法律上の守秘義務を負う者。

2.4.5. 第 2.15 条に従って、かかる協力、支援および情報を顧客に提供し、範囲内の個人データに関連する限りにおいてデータ保護法に基づく義務の遵守を支援することを合理的に要請できるすべての文書を実行すること、および

2.4.6. 当該データに関して監督当局の指示または決定を協力して遵守すること、いずれの場合も、顧客を支援し、データ保護法または監督当局が課す時間制限を満たす時間を超えないこと。

2.5. その処理に欧州連合または加盟国の法律が適用される範囲内の個人データに関して、サプライヤは、以下のとおり対応するものとします。

2.5.1. 次の場合を除き、いかなる国または地域からも当該データを移転せず、サブプロセッサーが当該データを移転しないように努め、顧客にかかる移転を行うように要求しないこと。

2.5.2. 欧州連合および欧州経済地域の加盟国間における場合。

2.5.3. 書面による顧客の指示に従い、顧客が設定した合理的な追加の制限に従う場合。この種類の移転に関連していつでも、顧客が合理的に規定できる方法、または両当事者が書面で合意できるその他の形式で履行される（改訂されていない）モデル条項に関するサプライヤとの合意をただちに締結すること（または、サブプロセッサーによる移転もしくはサブプロセッサーに対する移転の場合には、サブプロセッサーが速やかに合意を締結することを要求すること）。

2.6 第 2.5 条に該当しない範囲内の個人データの処理がデータ保護法の適用対象であって、当該データ保護法が (a) 当該範囲内の個人データを任意の国もしくは地域に移転すること、または (b) 当該範囲内の個人データを任意の国または地域で処理することを禁止または制限している場合、サプライヤは、かかる禁止または制限に違反して当該範囲内の個人データを移転または処理してはなりません。

2.7. サプライヤは、以下のとおり対応するものとします。

2.7.1. データ主体または監督当局から受けた問い合わせに対応するために顧客を支援する責任を負うサプライヤ担当者を常時配置すること（また、顧客のデータ保護担当者にその身元を書面で通知すること）。

2.7.2. 第 2.7.1 条で言及したサプライヤ担当者が、適時の対応に関す

るデータ保護法の関連要件を十分に考慮して、同条項で言及した問い合わせに常に迅速かつ合理的に対応すること。

2.7.3. 該当する顧客の書面による指示がある場合を除き、第 2.7.1 条で言及された問い合わせに関していかなる措置も講じないこと。

2.8. サプライヤは、以下のとおり対応するものとします。

2.8.1. いかなる範囲内の個人データも第三者に開示または移転しないこと。ただし、以下のいずれかの場合における開示または移転を除く。

2.8.2. 書面による顧客の指示に基づき、第 2.5 条に従って行われる場合。

2.8.3. データ保護法または本契約のその他の条項によって求められる場合。

2.8.4. サブプロセッサーによる範囲内の個人データの処理に関して、

(a) 第 13.2 条（譲渡、下請け）の規定に従うこと。

(b) 本別紙 3（データの保護：GDPR）に基づきサプライヤに課される義務と同様の義務をサブプロセッサーに課す書面による契約に基づいて、サブプロセッサーの処理が行われるように努めること。

(c) サブプロセッサーが義務を履行し、遵守するように努めること。

(d) 顧客の要請に応じて、サブプロセッサーが本別紙 3（データの保護：GDPR）に基づきサプライヤに課されている義務と同様の義務をサブプロセッサーに課す書面による契約を顧客と締結するように努めること。

2.9 サプライヤは、以下のとおり対応するものとします。

2.9.1. データ保護措置の一環として、範囲内の個人データへの不正または偶発的なアクセス、破壊、紛失、変更、使用または開示を防止するためのセキュリティ手順および慣行を含むデータ保護措置を採用、実施、および維持すること。

2.9.2. データ保護法に基づくサプライヤのデータセキュリティ義務に準拠した書面によるセキュリティポリシー、手順、および慣行を有していることを顧客に保証すること。

2.9.3. サプライヤが本サービスを提供する各施設において、また範囲内の個人データを処理するすべてのネットワークに関して、データ保護措置を維持し、実施すること。

2.9.4. 一般的な業界慣行に従って、また顧客の合理的な要請に応じて、データ保護措置を随時見直し、改訂すること（また、改訂されたデータ保護措置の詳細を要請に応じて速やかに顧客に書面で提供すること）。

2.10. 範囲内の個人データの不正もしくは偶発的なアクセス、使用、もしくは開示が生じた場合、または当該アクセス、使用、もしくは開示が発生した、もしくは発生する危険性があるとサプライヤが合理的に判断した場合（範囲内の個人データが存在しているもしくは保存されている可能性のある媒体、デバイス、もしくは機器を紛失した場合、またはこれらを明らかに特定できない場合などを含む）、サプライヤは、以下のとおり対応するものとします。

2.10.1. 遅滞なく、いかなる場合も 24 時間以内に顧客に通知し、当該アクセス、使用、または開示による顧客への影響、およびサプライヤが講じたまたは講じる予定の是正措置に関する合理的な説明を行うこと。

2.10.2. 第 2.15 条に基づき、当該アクセス、使用、または開示の根本原因を是正するために必要なすべての適切な是正措置を速やかに講じること。

2.10.3. データ保護法で求められているか否かを問わず、顧客の要請に応じて、影響を受けた可能性のあるデータ主体に通知することなどを含め、データ保護法によって求められる当該アクセス、使用、または開示に関するあらゆる措置を講じること。

2.10.4. 当該アクセス、使用、または開示によって、データ主体の財務情報へのアクセスが可能となる場合、または個人情報の盗難や不正行為の合理的な危険性につながる場合、サプライヤは、当該データ主体の信用モニタリングサービスを 1 年以上の合理的な期間にわたって提供すること。

2.11. 本契約の下での監査権に加え、また顧客による要請および顧客の合理的な裁量により、サプライヤは、本別紙 3（データの保護：GDPR）、データ保護法および顧客または顧客のクライアントの義務に対する準拠を検証するため、顧客（自身で、またはクライアントに代わり）、または顧客の指示を受けた独立監査人が、サプライヤまたは承認を受けたサブプロセッサーの情報セキュリティプログラム、データ処理設備およびデータ保護準拠プログラムの監査および審査を行うことを許可します（「データの保護および監査」）。

2.12. かかるデータの保護および監査には、サプライヤの、または承認を受けたサブプロセッサーの情報セキュリティプログラムおよび関連するセキュリティ措置（セキュリティ侵入テストを含む）に対する違反を検証するためのテストが含まれる場合があり、10 日前までの事前通知をもって行われるものとします。

2.13. データの保護および監査の結果により、サプライヤまたはサブプロセッサーが採用しているセキュリティ措置の脆弱性が特定されたと顧客が合理的に考える場合、サプライヤは、顧客の合意する期間内に、かかる脆弱性を評価し、顧客が満足する適切な解決策を提供するものとします。

2.14. サプライヤは、規制者またはその代理人がサプライヤまたは承認されたサブプロセッサーに対する監査を随時行うことができ、かかる監査は、2.11、2.12、2.13 および 2.14 の各条項に規定された制約の対象とはならないことを認めます。

2.15. 顧客は、以下のとおり対応するものとします。

2.15.1. 独自の権限によって、顧客に代わって個人データを処理する際に本契約に基づくサプライヤの義務の履行に合理的に必要な措置を講じることをサプライヤに指示する責任を負い、

2.15.2. データ保護法により許可されている範囲内で、サプライヤが顧客に代わってサブプロセッサーに同等の指示を与えることを許可します。

2.16. サプライヤに生じる費用および経費については、第 2.4 条、2.10.2 条、2.10.3 条および 2.10.4 条に従い、

2.16.1. サプライヤが講じる必要のある措置が、本契約の違反または GDPR の不遵守を含むサプライヤによる何らかの過失、故意もしくは不正による行為または不作為、サブプロセッサーもしくはサプライヤ要員に起因する場合には、サプライヤの負担とし、

2.16.2. これ以外の場合には、顧客の負担とします。

2.17. サプライヤは、随時、顧客の要請により、顧客が唯一のデータコントローラであり、本契約の下で顧客に代わりサプライヤが処理するすべての個人データを顧客に返却し、および/または顧客の要請により、かかる個人データをそのシステムから削除するものとします。ただし、適用される法律または規制の要件に準拠するため、サプライヤまたはその関連会社がそのバックアップコピーを保持することを要求される場合を除きます。この場合、かかるコピーは機密に、かつ本別紙 3（データの保護）に準じて安全に保管されることを条件とします。

サプライヤの代表者による署名

署名 _____

記名 _____

役職 _____

サプライヤ名 _____

日付 _____