EU 標準契約条項に基づくデータ処理契約(DPA)

株式会社コミュニケーションビジネスアヴェニュー

神奈川県横須賀市光の丘３番４号
YRP(横須賀リサーチパーク)センター1 番館 5F

（以下「CBA」という）

および

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
（以下「お客様」という）

前文
本注文処理（以下「DPA」という）は、株式会社コミュニケーションビジネスアヴェニュー（以下「処理者」という）とお客様（以下「管理者」という）間のマスターサブスクリプション契約（以下「MSA」という）の一部を構成するものです。本 DPA は、EU 標準契約条項（以下「EU SCC」という）に基づき作成されたものです。

1. 契約の構成要素

契約の一部は、本契約書本文および EU 標準契約条項で構成されます。

- 第１部　一般
- 第２部　当事者の義務
- 第３部　最終規定

および

- 附属１　当事者リスト
- 附属２　処理の詳細
- 附属３　データの安全性を確保するための技術的および組織的措置
- 附属４　副処理者リスト

2. 標準契約約款の補足事項

2.1 監査の証拠と費用
標準契約条項の第 7.6 項に従い、処理者は標準契約条項の遵守を証明するものを提出します。CBA はこれに対する報酬を要求する権利を有します。報酬は事前に合意しておきます。CBA は監査に先立ち、お客様に提案を行います。報酬のレートはいかなる場合においても、IT サービスにおける慣習的な報酬レートや MSA 第 1.13 条に準じた報酬レートを超えるこ

とはできません。サービスプロバイダーにおける監査費用などの外部費用は、お客様が全額を負担します。

データ保護監査権の以下の証拠は無償で提供されます。

- 一般データ保護規則第 40 条に基づき承認された行動規範の遵守
- 一般データ保護規則第 42 条に基づき承認された認証手順に従った認証
- 独立した機関（監査人、監査、データ保護担当者、IT セキュリティ部門、データ保護監査人、品質監査人など）からの現在の証明書、報告書または報告書の抜粋。
- IT セキュリティまたはデータ保護監査人による適切な証明書

2023 年　月　日

_____ CBA

_____ お客様

標準契約条項

第１部　一般

第１条

目的と範囲

a) 本標準契約条項（以下「本条項」という）の目的は、個人データの処理に関する自然人の保護および当該データの自由な移動に関する 2016 年 4 月 27 日の欧州議会および理事会の規則 (EU) 2016/679 第 28 条 (3) と (4)、並びに指令 95/46/EC（一般データ保護規則）を確実に遵守することです。

b) 附属 1 に記載されている管理者と処理者は、規則 (EU)2016/679 の第 28 条 (3) と (4)、および/または規則 (EU) 2018/1725 の第 29 条 (3) と (4) を確実に順守するため、本条項に同意します。

c) 本条項は、附属書類 2 に規定される個人データの処理に適用されます。

d) 附属 2 から 4 は、本条項の不可欠な部分です。

e) 本条項は、規則 (EU) 2016/679 および/または規則 (EU) 2018/1725 により管理者が従う義務を妨げるものではありません。

f) 本条項は、それ自体、規則 (EU) 2016/679 および/または規則 (EU) 2018/1725 第 5 章に従った国際移転に関連する義務の遵守を保証するものではありません。

第２条

条項の不変性

a) 当事者は，附属の情報の追加または更新を除き，本条項を変更しないことを約束します。

b) これは両当事者が、より広範な契約において本条項で規定される標準契約条項を含めること、直接的または間接的に本条項と矛盾しないことや、データ主体の基本的権利または自由を損なわないことを条件として、他の条項や保護措置を追加することを妨げるものではありません。

第３条

解釈

a) 本条項が規則 (EU)2 016/679 または規則 (EU) 2018/1725 で定義されている用語を使用している場合、それらの用語はその規則と同じ意味を有します。

b) 本条項はそれぞれ規則 (EU) 2016/679 または規則 (EU) 2018/1725 の規定に照らして読まれ、解釈します。

c) 本条項は、規則 (EU) 2016/679 および規則 (EU) 2018/1725 に規定される権利および義務に反する形で、またはデータ主体の基本的権利または自由を害する形で解釈されることはありません。

第 4 条

優先度

本条項と、本条項が合意またはその後締結された時点で存在する当事者間の関連契約の規定との間に矛盾がある場合には、本条項が優先するものとします。

第 5 条　オプション

結合条項

a) 本条項の当事者でないいかなる事業者も、当事者の同意を得て附属に記入され、附属 1 に署名することにより、管理者または処理者としていつでも本条項に加盟することができます。

b) (a) の附属に記載され署名した場合、加盟事業者は、附属 1 の指定に従って本条項の当事者として扱われ、管理者または処理者の権利および義務を有します。

c) 加盟する事業者は、本条項の当事者となる前の期間から生じる、本条項に起因するいかなる権利または義務も有しません。

第 2 部　当事者の義務

第 6 条

処理の内容

処理業務の詳細、特に管理者に代わって個人データを取り扱う場合における個人データの種類と処理目的は、附属 2 に明記されています。

第 7 条

当事者の義務

7.1 指示

a) 処理者は、処理者が従うべき連邦法または加盟国法によって要求されない限り、管理者からの文書化された指示に基づいてのみ個人データを取り扱います。この場合、処理者は、公共の利益という重要な理由で法律がこれを禁止している場合を除き、処理前に当該法的要件を管理者に通知します。また、個人データの処理期間を通じて、管理者から事後の指示が与えられる場合があります。これらの指示は常に文書化されるものとします。

b) 処理者は、管理者が与えた指示が規則 (EU) 2016/679 および規則 (EU) 2018/1725、または適用される EU または加盟国のデータ保護規定を侵害していると考える場合、直ちに管理者に通知します。

7.2 目的の制限

処理者は、管理者から更なる指示を受けない限り、附属 2 に記載された特定の目的のためにのみ個人データを取り扱います。

7.3 個人データの処理期間

処理者による取り扱いは、附属 2 に明記された期間のみ行われます。

7.4 処理の安全性

a) 処理者は、個人データの安全性を確保するため、少なくとも附属 3 に規定されている技術的および組織的な措置を実施します。これには、偶発的または違法な破壊、紛失、改ざん、不正な開示またはデータへのアクセスにつながるセキュリティ違反（個人情報の漏えい）に対するデータの保護が含まれます。適切な安全レベルを評価する際、両当事者は、技術の現状、導入のコスト、処理の性質、範囲、文脈および目的並びにデータ対象者に関わるリスクを十分に考慮します。

b) 処理者は、契約の実施、管理、および監視に厳密に必要な範囲でのみ、当該担当者に個人データへのアクセスを許可します。処理者は、個人データの処理を許可された者が守秘義務を負っている、または適切な法廷の守秘義務を負っていることを保証します。

7.5 センシティブデータ

情報の取り扱いに、人種または民族的出身、政治的意見、宗教上または哲学上の信条、労働組合への加入、自然人を一意に識別することを目的とする遺伝子データまたは生体データ、健康、性生活または性的指向に関するデータ、または犯罪歴および犯罪に関するデータ（以下「センシティブデータ」という）が含まれる場合、処理者は特定の制限および/または追加の保護措置を適用しなければなりません。

7.6 文書化および遵守

a) 当事者は、本条項を順守していることを証明できなければなりません。

b) 処理者は、本条項に従ったデータ処理に関する管理者からの問い合わせに迅速かつ適切に対処します。

c) 処理者は、本条項で規定され、規則 (EU) 2016/679 および/または規則 (EU) 2018/1725 に直接起因する義務の遵守を実証するために必要なすべての情報を管理者に提供します。処理者は管理者の要求に応じて、合理的な間隔で、または非遵守の兆候がある場合には本条項が対象とする処理活動の監査を許可し、これに協力するものとします。管理者は、審査または監査を決定する際、処理者が保有する関連する認定を考慮することができます。

d) 管理者は、独自に監査を実施するか、独立監査人に委任するかを選択することができます。監査には、処理者の敷地または物理的施設における検査も含まれることがあり、合理的な通知をもって実施されるものとします。

e) 当事者は、監査の結果を含め本条項で規定されている情報を、要求に応じて管轄の監督当局/機関に提供します。

7.7 副処理者の使用

a) 書面による一般的な許可。処理者は、合意されたリストの中から副処理者を選択することについて、管理者の一般的な許可を得ています。情報処理者は、副処理者の追加または交換により当該リストを変更する場合、少なくとも 4 週間前に書面にて通知し、これにより当該副処理者の採用前に、管理者が当該変更に異議を唱える機会を確保します。処理者は、管理者が異議を唱える権利を行使するために必要な情報を管理者に提供します。

b) 処理者が（管理者に代わって）特定の処理を実施するために副処理者を利用する場合、本条項に従ってデータ処理者に課される義務と実質的に同じデータ保護義務を、契約によって副処理者に課するものとします。処理者は、本条項ならびに規則 (EU) 2016/679 および/または規定 (EU) 2018/1725 に基づき、処理者が負う義務を副処理者が遵守することを保証します。

c) 処理者は、管理者の要求があった場合、当該副処理者契約およびその後の改訂版のコピーを管理者に提供します。個人データを含む事業上の秘密またはその他の機密情報を保護するために必要な範囲において、処理者はコピーを共有する前に契約書の本文を修正することができます。

d) 処理者は、処理者と副処理者との間の契約に基づく副処理者の義務の履行について、管理者に対し完全な責任を負います。処理者は、副処理者が契約上の義務を履行できない場合、管理者に通知します。

e) 処理者は、副処理者と第三者受益権条項に合意します。これにより、処理者が事実上消滅した場合、法律上消滅した場合、または支払不能に陥った場合、管理者が副処理者との契約を解除し、副処理者に個人情報の消去または返却を指示する権利を有するものとします。

7.8 国際的な移転

a) 処理者による第三国または国際機関へのデータの移転は、管理者からの文書化された指示に基づき、または処理者が従う EU または加盟国の法律に基づく特定の要件を満たすためにのみ行われ、規則 (EU) 2016/679 の第 5 章または規則 (EU) 2018/1725 を遵守するものとします。

b) 管理者は、処理者が（管理者に代わって）特定の処理を実施するために第 7.7 条に従って副処理者を利用し、それらの処理が規則 (EU) 2016/679 第 5 章の意味における個人デ

ータの移転を伴う場合、処理者および副処理者が規則 (EU) 2016/679 第 46 条 (2) に従って欧州委員会が採択した標準契約条項を使用することにより、規則 (EU) 2016/679 第 5 章の遵守を保証できることに同意します。ただし、これらの標準契約条項の使用条件を満たしている場合に限ります。

第 8 条

管理者への支援

a) 処理者は、データ対象者から受け取った要求について、速やかに管理者に通知するものとします。処理者は、管理者から権限を付与されない限り、その要求に自ら回答しません。

b) 処理者は、データ主体の権利行使の要求に対応する義務を、処理の性質に配慮して管理者が果たすことを支援するものとします。(a) および (b) に従った義務を果たすにあたり、処理者は管理者の指示に従います。

c) 処理者は、第 8 条 (b) に基づく管理者の支援義務に加え、データ処理の性質および処理者が利用できる情報を考慮し、以下の義務を確実に遵守するために管理者をさらに支援するものとします。

   1) ある種の処理が自然人の権利と自由に対して高い危険性をもたらす可能性がある場合、想定される処理操作が個人情報の保護に与える影響の評価（以下「データ保護影響評価」という）を実施する義務。

   2) データ保護影響評価により、管理者が危険性を軽減するための措置を講じず当該処理の危険性が高くなることが示された場合、処理前に管轄の監督官庁に相談する義務。

   3) 処理者が処理中の個人情報が不正確または古くなっていることを認識した場合、遅滞なく管理者に通知することにより、個人情報の正確性および最新性を確保する義務。

   4) 規則 (EU) 2016/679 第 32 条に定める義務。

d) 当事者は、本条項の適用において処理者が管理者を支援するために必要とされる適切な技術的および組織的措置、並びに必要とされる支援の範囲および程度を附属 3 に定めます。

第 9 条

個人情報漏えいに関する通知

個人データの漏えいが発生した場合、処理者は、処理の性質および処理者が利用可能な情報を考慮し、該当する場合、規則 (EU) 2016/679 第 33 条と第 34 条に基づく義務、または規則 (EU) 2018/1725 の第 34 条と第 35 条に基づく義務を管理者が遵守するために協力し支援します。

9.1 管理者が処理するデータに関するデータ漏えい

管理者が取り扱うデータに関して個人情報の漏えいが発生した場合、処理者は管理者を支援します。

a) 管理者は個人情報漏えいに気付いた後、管轄の監督当局に不当な遅滞なく通知します（個人情報漏えいが自然人の権利と自由に対するリスクをもたらす可能性が低い場合を除く）。

b) 規則 (EU) 2016/679 の第 33 条 (3) に基づき、管理者の通知に記載されなければならず、少なくとも含まれなければならない以下の情報を取得します。

   1) 可能であれば、関係するデータ主体の種類と概数、関係する個人データ記録の種類と概数を含む、個人データの性質。

   2) 個人情報漏えいから起こり得る結果。

   3) 個人情報漏えいに対処するために管理者が講じた、または提案した措置（適切な場合には、その起こり得る悪影響を軽減するための措置を含む）。

これらすべての情報を同時に提供することが不可能な場合、最初の通知にはその時点で入手可能な情報が含まれ、その後入手可能になり次第さらなる情報を遅滞なく提供します。

c) 規則 (EU) 2016/679 第 34 条に基づき、個人データの侵害が自然人の権利と自由に対する高いリスクをもたらす可能性がある場合、データ対象者に個人データの侵害を不当に遅滞なく伝達する義務を遵守すること。

9.2 処理者が処理するデータに関するデータ漏えい

処理者が処理したデータに関して個人情報の漏えいが発生した場合、処理者はその漏えいを認識した後、不当な遅滞なく管理者に通知します。当該通知には少なくとも以下の内容が含まれます。

a) 違反の性質の説明（可能であれば、関係するデータ対象者およびデータ記録の種類と概数を含む）。

b) 個人情報漏えいに関する詳細な情報を入手できる連絡先の詳細。

c) 違反に対処するために講じた、または提案された措置（起こりうる悪影響を軽減するための措置を含む）。

これらすべての情報を同時に提供することが不可能な場合、最初の通知にはその時点で入手可能な情報が含まれ、その後入手可能になり次第さらなる情報を遅滞なく提供します。
当事者は、規制 (EU) 2016/679 第 33 条と第 34 条にある、管理者の義務の遵守を支援する際に処理者が提供すべき他のすべての要素を附属 3 に定めるものとします。

第 3 部　最終規定

第 10 条

本条項の不遵守と解除

a) 規則 (EU) 2016/679 および/または規則 (EU) 2018/1725 の規定を妨げることなく、処理者が本条項による義務に違反している場合、管理者は処理者が本条項を遵守するか契約が終了するまで個人情報の処理を一時停止するよう指示することができます。処理者が本条項を遵守できない場合、理由の如何を問わず、迅速に管理者に通知します。

b) 管理者は、以下の場合、本条項に従った個人情報の処理に関する限り、契約を終了する権利を有するものとします。

1) 管理者が (a) 項に従い処理者による個人情報の処理を一時停止し、かつ本条項の遵守が合理的な時間内に、いかなる場合でも停止後 1 カ月以内に回復されない場合。

2) 処理者が、本条項または規則 (EU) 2016/679 および/または規則 (EU) 2018/1725 に基づく義務に実質的または継続的に違反している場合。

3) 処理者が、本条項または規則 (EU) 2016/679 および/または規則 (EU) 2018/1725 に基づく義務に関して、管轄裁判所または管轄監督当局/機関の拘束力のある決定を遵守しない場合。

a) 処理者は、その指示が第 7.1 条 (b) 項に従って適用される法的要件を侵害することを管理者に通知した後、管理者がその指示の遵守を主張した場合、本条項に基づく個人データの処理に関してのみ、契約を解除する権利を有します。

b) 契約の解除後、処理者は、管理者の選択により、管理者に代わって処理されたすべての個人データを削除し、管理者に削除したことを証明するか、または、すべての個人データを管理者に返却し、連合法または加盟国の法令により個人データの保存が要求されない限り、既存のコピーを削除します。データが削除または返却されるまで、処理者は本条項の遵守を引き続き保証するものとします。

附属１　当事者リスト

管理者（管理者の身元および連絡先の詳細、該当する場合は管理者のデータ保護責任者）

1. 氏名

住所

連絡先の担当者の氏名、役職、連絡先の詳細

署名と日付

2. 氏名

住所

連絡先の担当者の氏名、役職、連絡先の詳細

署名と日付

処理者（処理者の身元および連絡先の詳細、該当する場合は処理者のデータ保護責任者）

1. 氏名　株式会社コミュニケーションビジネスアヴェニュー

住所　神奈川県横須賀市光の丘３番４号　YRP(横須賀リサーチパーク)センター1番館 5F

連絡先の担当者の氏名、役職、連絡先の詳細
柴山 浩（CEO）　hiroshiba@cba-japan.com

署名と日付：2023 年　月　日

2. 氏名　株式会社コミュニケーションビジネスアヴェニュー

住所　神奈川県横須賀市光の丘３番４号　YRP(横須賀リサーチパーク)センター1番館 5F

連絡先の担当者の氏名、役職、連絡先の詳細
岡村 洋一郎（CIO）　okamura@cba-japan.com

署名と日付：2023 年　月　日

附属２　処理の詳細

個人データを処理されるデータ主体の種類

当社にサービスを依頼するあらゆる種類の顧客、消費者、企業のビジネスパートナー。

処理される個人データの種類

メールアドレスやその他の連絡先が、個人データとして本サービスに保存されることがあります。当社は、本サービスにおいて、通常の業務および本サービスの利用において必要とされる個人データのみを保存または記録する義務を負います。

処理の性質およびセンシティブデータ処理に関する情報提供

クラウドアプリケーションの一部として、本サービスは、電子メール、文書、音声録音、テキストメッセージ、あらゆる種類の添付ファイル、チャット、名前およびその他のサービスデータを処理します。この文脈で、個人データは、当社が本サービスに保存することができます。
当社は、本サービスに保存される個人データを自ら管理することができます。会社が本サービスに保存することを希望する正確なデータは CBA に知らされず、暗号化された形で保存されます。CBA は以下について一切の情報を持っていません。

a) どのようなサービスデータが格納されているか
b) サービスデータにはどのような個人データが含まれるか
c) センシティブデータの取り扱いの有無

処理期間

当社の個人データの処理期間は、主契約および本委託処理に規定されています。

附属 3　データの安全性を確保するための技術的・組織的措置

CBA は、データ保護とデータ安全性の法的要件に基づき、お客様のデータを誤用や損失から適切に保護するための技術的・組織的な措置を講じます。これらはデータの安全対策であり、システムの機密性、完全性、可用性、弾力性の観点からリスクに見合った保護レベルを確保するためのものです。この文脈では、最新技術、導入コスト、処理の性質、範囲、目的、および DS-GVO 第 32 条 1 項の意味における自然人の権利と自由に対するリスクの様々な可能性と重大性が考慮されます。特に、CBA はデータ保護の特定の要件を満たすように内部組織を設計しています。これらについては以下で詳しく説明します。
必須の事前サービスは、データセンターオペレーター（下請け業者）により提供されます。このため、前述のプロバイダーはそれぞれ、契約期間中に適切な技術的・組織的データ保護措置を維持することを CBA に契約で保証しています。
以下に説明する措置は、企業データへのアクセスに関するセキュリティリスクを最小化し、それに対応する企業および事業上の秘密を保護するため、とりわけ安全上の理由から、詳細には開示されません。GDPR 第 32 条の規定を満たすための基本要件としてのみ機能します。

1.　機密保持（DS-GVO 第 32 条 1 項 b 号）

a)　アクセス制御

*不正アクセスは防止しなければならないが、この用語は空間的に理解されなければならない。*アクセス制御のための技術的または組織的な手段、特に許可された者の正当性を証明するための手段。

技術的措置	組織的措置
警報装置	鍵の管理・文書化・鍵の割り当て
ビル、オフィスフロア、個別に保護されたオフィスルームへの生体認証アクセス制御	訪問者の履歴を記録
ビルシャフトの保護	ビルシャフトの保護
カメラ付き警報システム	サービスプロバイダーやパートナーの選定に配慮（サプライヤー・セキュリティ・ディレクティブ）
安全ガラス	
強化ドアと生体認証またはロックシステムで保護されたサーバールーム	
モーションディテクター	

独立した建物へのアクセスは、警報システムの生体認証解除と適切な認証を受けたアクセス（指紋）でのみ可能です（通常の営業時間外でも、夜間のロックダウン期間中は不可）。
セキュリティレベルに応じて、個々のセキュリティエリア内に追加の指紋スキャナーが用意されています。
通常の営業時間内は、訪問者は訪問者リストに記録され、対応する機密保持契約は訪問者の署名によって書面で受理されます。

b)　アクセス制御

データ処理システムへの権限のない者の侵入を防がなければならない。

技術的措置	組織的措置
ユーザー名＋パスワードでログイン	ユーザープロファイルの作成と管理
アンチウィルスソフトウェアサーバー	ユーザー権限の作成と管理
アンチウィルスソフトウェアクライアント	ユーザーパスワード管理
ファイアウォール	セキュアパスワードポリシー
リモートアクセスに VPN を使用	クリーンデスク/クリアスクリーンポリシー
重要な IT システムの監視	ポリシー ”電子メールとインターネットの利用について”
	情報セキュリティポリシー
	プライバシーポリシー

ネットワーク内のクライアントシステムへのアクセスは、パスワードで保護されたネットワーク認証を経由してのみ可能です。外部からの直接アクセス（ネットワーク外からのアクセス）は、安全で暗号化された接続と、会社が提供するコンピューター/ラップトップ（または同様のハードウェア）を介してのみ可能です。第三者のシステムへの安全なアクセスには、ファイアウォールとプロキシサーバーが使用されます。

c) アクセス制御

DP システムにおいて、与えられた権限以外の不正な活動は防止しなければならない。

技術的措置	組織的措置
ユーザーID＋パスワード	認可の概念
アプリケーションへのアクセス、特にデータの入力、変更、削除の履歴を残す	管理者によるユーザー権限の管理
ファイルシュレッダー（レベル 3 以上、クロスカット）	アクセス権の定期的な見直し
社外文書廃棄	従業員の入社・退社手順
	アクセス制御指令
	ローカル・アドミニストレイティブ・ライツ・ディレクティブ

これは、すべての IT システムに関して、ユーザープロファイルとロールの定義に対応した認可の概念に基づいています。権限付与は、「最小権限」の原則に従って行われます。つまり、ユーザーは各自のタスクを実行するために必要な IT システムの権限のみを受け取ることができます。アクセスは常に、ユーザーID とパスワードを持つユーザーアカウントを介して行われます。アクセスは、関連するサーバー上のログ・エントリーによって記録されます。

d) 分離管理

異なる目的のために収集されたデータも、別々に処理されるものとする。

技術的措置	組織的措置
関連アプリケーションのマルチクライアント対応	機能の分離
フォルダー構造の分離（受注処理）	認可概念による制御
	データベースの権限設定

すべての従業員は、サービス提供の範囲内においてのみ、目的の制限を遵守して個人データを収集、処理または利用するよう指導および訓練されています。

2. 完全性（DS-GVO 第 32 条 1 項 b 号）

a) 移転管理

個人データを電子的に送信中、またはデータ媒体に伝送もしくは保存されている間に、権限のない者によって読み取り、コピー、変更または削除されないことを保証し、データ送信装置によって個人データがどのような団体に送信される予定であるかを確認および判断することを可能とするための措置。

技術的措置	組織的措置
トンネル接続（VPN）	情報セキュリティポリシー
ハイブリッド暗号化プロトコル TLS	密封包装または容器
ファイアウォール	
アクセス・検索の履歴を取得	

IT システムからの個人データの受け渡しは、原則として行いません。該当する法的または契約上の根拠に基づいて移転が許可された場合は、関連会社、顧客、パートナー、サプライヤーに移転されることがあります。データの移転は、それぞれの第三者との間で機密保持契約および注文処理契約を締結することによって確保されなければなりません。

b) 入力管理

データの管理と保守のトレーサビリティまたは文書化が確保されるものとする。

技術的措置	組織的措置
データの入力、変更、削除の技術的な履歴	データの入力、変更、削除を個々のユーザー名で追跡可能（ユーザーグループではない）
	認可概念に基づくデータの入力、変更、削除の権利の割り当て

3. 可用性と回復力（DS-GVO 第 32 条 1 項 b 号）

a) 可用性の管理

データは、不慮の破壊や損失から保護されなければならない。

技術的措置	組織的措置
火災・煙感知システム	緊急時対応計画
消火器	バックアップの手順
サーバールーム空調完備	復旧手順
米軍	
ファイアウォール、アンチウィルスプログラム	
定期的なバックアップ	

4. 定期的なレビュー、アセスメント、評価のための手順（GDPR 第 32 条 1 項 d 号、同第 25 条 1 項）

個人情報の保護に関する GDPR の要求事項への適合性を継続的に見直し、評価・査定するために、以下のような対策をとっています。

a) データ保護管理

技術的措置	組織的措置
データ保護管理のためのソフトウェアソリューションの活用	データ保護責任者

データ保護に関するすべての手順と規則を一元的に文書化し、従業員が必要性や権限に応じてアクセスできるようにする。	データ保護担当者への定期的なトレーニング
	従業員への教育、機密保持・データセキュリティの徹底
	従業員への定期的な啓蒙活動
	必要に応じたデータ保護影響評価の実施
	DS-GVO 第 13 条および第 14 条に基づく情報義務の遵守
	従業員は DS-GVO に基づくデータ保護要件を遵守する義務あり

b) インシデントレスポンス管理

技術的措置	**組織的措置**
ファイアウォールの使用と定期的な更新	セキュリティインシデント/データ漏えいを検出し報告するための手順を文書化
スパムフィルターの使用と定期的な更新	セキュリティ事故およびデータ漏えいに対するデータ保護責任者の関与
ウイルススキャナーの使用と定期的な更新	チケットシステムによるセキュリティインシデントおよびデータ漏えいの文書化

c) データ保護に配慮した初期設定（GDPR 第 25 条 2 項）

技術的措置	**組織的措置**
それぞれの目的に必要な個人情報のみを収集	
技術的手段によるデータ主体の撤回権の簡易執行	

d) 注文の管理

DS-GVO 第 28 条に規定されるデータ処理の委託を受けないこと。DS-GVO 第 28 条に規定されたデータ処理を、顧客からの指示なしに行わないこと（例：明確な契約設計、形式的な受注管理、サービス提供者の厳格な選定、事前の説得義務、フォローアップの確認など）。

技術的措置	**組織的措置**
	サプライヤーセキュリティディレクティブ
	下請け業者が行った安全対策とその資料の事前検証
	特にデータ保護とデータセキュリティに関する慎重な委託先の選定を
	委託処理に関する必要な契約または EU 標準契約条項の締結
	下請け業者の従業員のデータ機密保持義務
	契約者によるデータ保護責任者の選任義務が発生した場合

	更なる下請け業者の使用に関する規制
	注文完了後のデータ破棄・返却の確認

附属 4　副処理者リスト

副処理者	目的	データ保存
German Edge Cloud GmbH & Co. KG Düsseldorfer Straße 40 a, 65760, Eschborn, Deutschland	クラウド EU ThinkOwl Europe 環境のホスティングと運用	EU
ITyX Technology GmbH Carl-Benz-Straße 10-12, 56218 Mülheim-Kärlich, Deutschland	ソフトウェアサポート、セールスサポート、DE ThinkOwl Europe プロジェクト管理、Microsoft Office 365、Web ページプロバイダ (すべてドイツ)。	ドイツ
fileee GmbH Windthorstraße 68, 48143 Münster, Deutschland	ThinkOwl のお客様に対し fileee の会話を使用可能とする	ドイツ
Amazon Web Services Inc. 38 avenue John F. Kennedy, L-1855, Luxemburg	ThinkOwl Europe の主要なクラウド・インフラストラクチャーのプロバイダーで、添付ファイルを含むメールが保存される場所。バックアップの保管場所（暗号化）。	ドイツ
Amazon Web Services Inc. 38 avenue John F. Kennedy, L-1855, Luxemburg	ThinkOwl のメールアドレスでメールを送受信する際、メールが取り込まれるまでの一時的な保管場所	アイルランド
Zendesk (元 Smooch.io) 5333 Casgrain, Suite 1201, Montreal, QC, H2T1X3 Canada	ThinkOwl のお客様に対し、ThinkOwl のアカウントを Whatsapp for Business と統合可能にする	EU
Cloudflare 101 Townsend St., San Francisco, California 94107, USA	ThinkOwl との間で送受信される Web トラフィックに DNS サービスを提供	全世界
Stripe Payments Europe ltd C/O A&L Goodbody, Ifsc, North Wall Quay, Dublin, Ireland	顧客からのライセンス料を決済するサービスを提供	アイルランド
Chargebee 340 S Lemon Avenue, #1537 Walnut, California 91789, USA	顧客からのライセンス料を決済するサービスを提供	EU/米国