データ処理規約

当事者:

お客様（以下「**データ管理者**」をいいます）

および

HCL America, Inc（以下「**データ処理者**」といいます）

上記当事者は、以下のとおり合意します。

1. データ処理規約の主題

1.1. このデータ処理規約は、EU データ保護法[i]の適用対象である個人データの処理（両当事者間で[期日]に発効する、[サービスの提供]（以下「本件サービス」といいます）についての契約（以下「本件契約」といいます）の範囲によるもの）に専ら適用されます。この規約は、本書によって参照方式で本契約に組み込まれ、本契約によって規律されます。

1.2. EU データ保護法という用語は、個人データの処理およびその自由な移動に関して、自然人を保護するために、指令（95/46/EC）を廃止して採択された、2016 年 4 月 27 日付の欧州議会および欧州理事会規則（（EU）2016／679）（一般データ保護規則）を意味します。

i 本書では EU モデルを想定していますが、サービスを提供する地域に応じて、その他の該当する法律が適用される場合があります。

1.3. 「処理する」、「個人データ」、「データ管理者」および「処理者」などの用語は、EU データ保護法で付与された意味を有するものとします。

1.4. データ処理者が、データ管理者との間の本件契約を履行する過程で、データ管理者のために EU データ保護法に従って個人データを処理する範囲で、本データ保護契約の条項が適用されます。個人データの分類、データ主体の種類、および個人データを処理する目的の概要は、添付書 2 に規定されています。

2. データ管理者およびデータ処理者

2.1. データ管理者は、データ処理者が個人データにアクセスし、それを処理する範囲、目的および方法を決めます。データ処理者は、データ管理者の書面による指示書に記載された範囲に限り、個人データを処理します。

2.2. データ処理者は、データ管理者の書面による指示書に基づいて、サービスの提供に適する方法、適する範囲に限り、個人データを処理します。ただし、データ処理者が服する法的義務を順守するのに必要な場合はその例外とします。こうした場合、データ処理者は、処理する前にそうした法的義務についてデータ管理者に知らせるものとします。ただし、法律により、データ管理者へのそうした情報の提供が明示的に禁じられている場合を除きます。データ処理者は、自身の見解により、指示が本規則を侵害していると考える場合、データ管理者に速やかに知らせるものとします。

2.3. 両当事者は、添付書 22 に定める目的で、個人データを保護し処理する処理者の専門知識から利益を得るために、本件契約を締結しました。データ処理者は、自身が上記の目的を追求するために必要と考える手段を選択しこれを用いる際に、本データ処理規約の要請に従うことを条件として、自身の指示内容を行使できるものとします。

2.4. データ管理者は、本件サービスに関して処理をおこなわせるにあたり、個人データをデータ処理者に提供するのに必要なすべての権利を有していることを保証します。適用のあるデータ保護法で要請される範囲で、データ管理者は、必要なデータ主体から、この処理に対する同意を得ていること、また、こうした同意の記録を維持していることを確認する責任を負います。データ主体がこうした同意を撤回した場合、データ管理者はその撤回についてデータ処理者に通知する責任を負うとともに、データ処理者は、当該個人データのその後の処理についてデータ管理者から指示があった場合には、その指示を実施することについて引き続き責任を負います。

3. 秘密保持

3.1. 下記は両当事者間の既存の契約上の取り決めに影響を与えるものではないですが、データ処理者は、すべての個人データを厳格に秘密として扱うとともに、個人データの処理に携わる自身のすべての従業員、代理業者、および／または認定下請け処理者に、個人データの秘密としての性質について、知らせるものとします。データ処理者は、こうした個人もしくは組織が適切な秘密保持契約に署名していること、秘密保持義務に拘束されていること、もしくは適切な制定法上の秘密保持義務を課されていることを確認するものとします。

4. セキュリティ [ii] [iii]

4.1. データ管理者とデータ処理者は、最新技術、処理の導入費用、および処理の性質、範囲、内容と目的、ならびに自然人の権利と自由に対する様々なリスクおよび重大性を考慮して、両当事者が合意しているその他のセキュリティ基準に加えて、適切な技術的、組織的対策を導入し、リスクに対応した個人データの処理について一定レベルのセキュリティレベルを確保するものとします。こうした対策には、場合に応じて、以下を含むものとします。

---

ii GDPR（欧州一般データ保護規則）第 32 条(3)項：第 40 条で言及される公認の行動規範、または第 42 条で言及される公認の認証メカニズムを順守している事実は、本条の第 1 項に定める要件の順守を実証するための要素として使用することができる。

iii 処理者は、認証を共有することで順守を実証することができる。

(a) 個人データを、本データ処理規約の添付書 2 に定めた目的のために、許可された人員に限りアクセス可能とするように確保する対策。

(b) セキュリティレベルが適切かどうかを審査するにあたり、処理において提示されたあらゆるリスク（例えば、個人データの偶発的、非合法的な破壊、喪失または改ざん、無許可のもしくは非合法的な保存・処理・アクセス・開示など）を特に考慮すること。

(c) 個人データの匿名化および暗号化。

(d) 処理システムおよび処理サービスの継続的な機密性、完全性、可用性および回復力を確保する能力。

(e) 物理的、技術的なインシデントが発生した際にタイムリーに個人データの可用性およびアクセスを回復する能力。

(f) 個人データの処理のセキュリティを確保するための技術的、組織的対策の効果を定期的に試験、審査、評価するプロセス。

(g) データ管理者にサービスを提供するのに使われるシステムにおいて、個人データ処理に関係する脆弱性を特定する措置。

(h) 添付書 3 に記載された、両当事者が合意した対策。

4.2. データ処理者は、個人データの処理に関して、第 4.1 項に定めた対策の概要を必ず記載した、書面によるセキュリティ方針を常に配備するものとします。

4.3. データ管理者からの要請に応じて、データ処理者は、第 4 条に従って講じている対策を実証して、上記の対策をデータ管理者が監査、試験できるようにするものとします。データ処理者は、データ管理者が個人データに関係したデータ処理者の施設と運用の監査を実行し、またはデータ処理者と秘密保持契約を締結している第三者にそれを実行させる際には、14 日以上の事前の通知を受ける権利を与えられるものとします。お客様は監査に関係して発生した自身の諸費用と諸経費をすべて負担するものとします。規制者が実施する監査を除き、監査は各暦年に 1 回を超えて実施することはできず、また監査実施の 14 日以上前に書面による通知を受けている必要があります。データ処理者は、データ管理者が実行する監査、またはデータ管理者を代理して実行される監査に協力するものとします。お客様は、サプライヤーが処理に関係する本契約の義務を順守しているかどうかを検証するために、お客様の個人データを処理するために使われるサプライヤーのシステムを監査する権利を与えられるものとします。いかなる監査も以下の条件に従うものとします。

i 監査を実施するために任命された第三者は、処理者またはその関連会社の競合者であってはならない。

ii. 処理者は、自身が合理的に満足する秘密保持契約を当該第三者が

締結していなければ、または締結するまでは、いかなる第三者に対しても、自身のシステム、設備、施設へのアクセスを許可するよう要求はされない。

iii. 監査の範囲は、個人データ処理に使われる処理者のシステム（またはそのようなシステムの部品）のみに厳格に限定される。

iv. 副条項(iii)の定めを制限するものではないが、管理者も第三者も、サプライヤーのその他の顧客、もしくはサプライヤーの内部費用や利益に関係するデータや情報にアクセスする権利は与えられないものとする。

5. セキュリティの改善

5.1. 両当事者は、セキュリティ要件は絶えず変化しており、効果的なセキュリティ要件にするためには、頻繁に評価し、また時代遅れのセキュリティ対策を定期的に改善する必要があることを確認します。したがって、データ処理者は、対策が第 4 条に準拠して導入されていることを継続的に評価し、また第 4 条に定めた要件の順守を維持するためにこうした対策を強化し、補足し、改善するものとします。両当事者は、適用のあるデータ保護法で定められた特定の更新されたセキュリティ要件によって必要となる重大な変更、または管轄権のあるデータ保護機関から要請された重大な変更を導入するための費用（もしあれば）について、誠実に交渉します。

5.2. 適用のあるデータ保護法の随時の変更による要請に応じてセキュリティ対策を改善するために、データ管理者からデータ処理者に出された指示を実行するのに本件契約の改定が必要な場合、両当事者は本件契約の改定について誠実に交渉するものとします。

6. データの転送

6.1. データ処理者は、適切な保護水準ではない欧州経済領域外の国に個人データを永久にもしくは一時的に転送する（または転送を予定する）場合、速やかにデータ管理者に通知するものとし、そうした（予定の）転送は、データ管理者から許可された場合にのみ実行するものとします。本件契約および本データ処理規約の締結時にデータ管理者が同意を与える転送のリストを、添付書 4 に記載します。

6.2. データ管理者またはデータ処理者が制定法上の特定のメカニズムに依拠して国際的なデータ転送を常態でおこなっていて、その後それが修正、廃止され、または管轄裁判所で無効と判断された場合、データ管理者およびデータ処理者は誠実に協力して、速やかに転送を終了するか、合法的に転送をサポートできる適切な代替メカニズムを探ることに合意します。

7. 通知の義務およびインシデント管理

7.1. データ処理者は本件サービス契約の対象である個人データの処理に影響を与えるインシデントに気付いた場合、速やかにデータ管理者に当該インシデントについて通知するものとし、いかなるときにもデータ管理者と協力するものとし、またこうしたインシデントに関係するデータ管理者の指示に従い、データ管理者がインシデントについて徹底的な調査を実施し、是正策を構築し、そしてインシデントに関係して適切な追加対策を講じられるようにするものとします。

7.2. 第 7.1 条で使われる「インシデント」という用語は、いかなる場合にも以下の意味を有するものと理解されるべきものとします。

(a) EU データ保護法に基づくデータ主体の権利の行使に関係する苦情もしくは要請。

(b) 政府職員による個人データの調査もしくは押収、またはそうした調査や押収が差し迫っている具体的な兆候。

(c) 個人データの無許可のもしくは偶発的なアクセス、処理、削除、喪失またはあらゆる形式の違法な処理。

(d) 本データ処理規約の第 3 条および第 4 条に記載されたセキュリティおよび／または秘密保持義務についての違反で、偶発的または違法な破壊、喪失、改ざんにつながるもの。個人データの無許可の開示もしくはアクセス。またはこうした違反が発生したこともしくは発生しそうなことを示す兆候。

(e) データ処理者の見解によれば、データ管理者から受けた指示を実施すると、データ管理者またはデータ処理者が服する適用法に違反することになる場合。

7.3. データ処理者は、インシデントについてデータ管理者に対して速やかに対応できるようにするための、書面による手順を常備しているものとします。適用のある EU データ保護法に基づき、データ管理者がデータ侵害通知をすることが要請される可能性が相当に高いインシデントの場合、データ処理者は、そうしたインシデントに気付いてから 72 時間以内にデータ管理者に通知できるようにするための手続書面を導入するものとします。

7.4. 第 7 条に従ってデータ管理者に通知する場合は、本データ処理規約の添付書 1 に連絡先情報が記載されるデータ管理者の従業員宛におこなうものとし、通知には以下を含めるものとします。

(a) 可能な場合、関連するデータ主体の分類と概数、および関連するデータ主体記録の分類と概数の説明。

(b) データ処理者のデータ保護責任者、もしくは詳細情報を得られる別の連絡窓口の氏名と連絡情報。

(c) インシデントによる潜在的な影響の説明。

(d) データ処理者がインシデントに対応するために講じる対策、または提案する対策、および場合に応じて、潜在的な悪影響を軽減するための対策の説明。

8. 下請け処理者への連絡

[データ管理者は、添付書 2 に記載のとおり、指定されたサービス関連活動をおこなう各国で下請け処理者を雇う権限をデータ処理者に与えます。

8.1. データ処理者は、下請け処理者が、本データ処理規約に基づくデータ処理者のデータ保護義務と同じ義務に拘束されるよう、確実を期するものとします。

8.2. データ管理者は、データ処理者に対し、第三者下請け処理者がデータ処理者から課された義務を本契約に準拠して順守していることを確保するために、第三者下請け処理者の監査を実施するように、またはこうした監査をすでに実施しているという確認を提供するように（もしくは、可能な場合、第三者下請け処理者の運営に関する第三者の監査報告を入手するか、顧客が入手するのを支援するように）要請できるものとします。

9. 個人データの返却または破棄

9.1. 本件契約および本データ処理規約の解除の時点で、またはデータ管理者から書面の要請を受けた時点で、または本サービスの中で合意されたすべての目的が履行されて、それ以上の処理の必要がなくなった時点で、データ処理者は、すべての個人データを削除、破棄、もしくはデータ管理者に返却し、かつ、既存のコピーを破棄または返却するものとします。

9.2. データ処理者は、自身の個人データの処理を支援しているすべての第三者に、本件契約および本データ処理規約の解除について通知するものとし、またすべての上記の第三者が、データ管理者の裁量に応じて、個人データを破棄するか、またはデータ管理者に返却するよう、確実を期するものとします。

10. データ管理者への支援

10.1. データ処理者は、可能な限り、適切な技術的および組織的対策を講じてデータ管理者を支援し、データ管理者が、GDPR に基づくデータ主体の権利を行使する要請に対応する義務を果たせるようにします。

10.2. データ処理者は、データ処理の性質およびデータで入手可能な情報を考慮して、データ管理者が第 4 条（セキュリティ）に基づく義務を確実に順守し、および GDPR 第 36 条に基づき要請される監督当局との事前協議を実施できるように支援するものとします。

10.3 データ処理者は、データ処理者の義務を順守していることを実証するために必要なすべての情報をデータ管理者に利用可能にするとともに、データ管理者もしくはデータ管理者が任命した他の監査人が実施する、検査を含めた監査を許可し、監査に貢献するものとします。

11. 期間および解除

11.1. 本データ処理規約は、データ処理者からデータ管理者に提供されるサポート、メンテナンスおよび／または専門サービスを規定する該当する本件契約の発効日の時点で効力を生じるものとします。

11.2. 本件契約および本データ処理規約の解除もしくは満了によって、データ処理者による第 3 条に基づく秘密保持義務が免除されることはありません。

11.3. データ処理者は、データ管理者から別途指示される場合を除き、もしくは当該データがデータ管理者からの指示に基づいて返却または破棄されるまでは、本件契約の解除日まで個人データを処理するものとします。

12. 雑則

12.1. 本データ処理規約の条項と、本件サービス契約の条項との間に不一致がある場合、本データ処理規約の条項が優先されるものとします。

12.2. データ管理者は、データ処理者を追加の関連リスクから保護するために、データ処理者が提案した本補遺に対す変更について、それへの同意を、不合理的に拒否したり、遅延したりしないものとします。データ管理者が、データ保護法の要件に対応するために必要と合理的に考えて、本補遺へのその他の変更を提案する場合、両当事者は速やかに提案された変更を協議し、お客様の通知の中で特定された要件に対

応するように考案されたそうした変更、もしくは、代替の変更について実際上できる限り早急に同意して実施することを目的として、誠実に交渉するものとします。

12.3. データ処理者は、データ主体の個人データに関連してデータ主体からデータ保護法に基づく要請を受けた場合、データ管理者に速やかにこれを通知するものとし、また契約した処理者が、お客様または関連するお客様の関連会社の文書による指示に基づく場合や適用法で要請される場合を除き、要請をしないように確保するものとします。こうした場合、データ処理者は適用法により許可される範囲で、データ管理者に法的要件を知らせてから、そうした要請に対応します。

12.4. 本データ処理規約には、個人データが処理される地である該当する加盟国の法律が適用されます。本データ処理規約に起因するか、それに関係する紛争は、個人データが処理される地である該当する加盟国内の管轄権のある裁判所の専属的な管轄に服するものとします。

12.5. 両当事者は、必要に応じて、以下の補遺を締結することに同意します。

添付書 1:

データ管理者の[データ保護責任者／コンプライアンス責任者]の連絡先情報

[連絡先情報]

データ処理者の[データ保護責任者／コンプライアンス責任者]の連絡先情報

[連絡先情報]

添付書 2:

本契約の範囲で処理される個人データおよび当該データの処理目的

添付書 3:

セキュリティ対策

添付書 4:

データ管理者が許可を与えている適切な保護レベルのない、欧州経済地域外の国への転送。