**データ共有に関する追加条項（会社データ）**

**改訂日：2024年3月12日**

本データ共有に関する追加条項（以下「本DSA」といいます。）において、「当社」とは、Merck Sharp & Dohme LLCまたはその関連会社であって、本DSAを参照する、契約またはその他の形式の合意（以下「本契約」といいます。）の締結主体となる法人のことを指し、本契約のその他の当事者すべてを総称して「サプライヤー」と呼ぶものとします。当社およびサプライヤーをそれぞれ「当事者」といい、合わせて「両当事者」といいます。

背景事情

1. 両当事者は本契約を締結したものであり、本契約に沿って、本契約において予定されている各種サービス（以下「本データ共有目的」といいます。）を管理する、単一または複数の注文書、発注書、プロジェクト契約書、プロジェクト計画の追加条項、作業明細書、作業指示書、またはその他のサービス条件（以下それぞれ「本作業明細書」といいます）を締結することができます。
2. 両当事者は、本契約に関連するすべての個人データの共有がデータ保護法に従って確実に実行されるように、本契約の条件を補足すること、および、サプライヤーが当該データの独立した管理者であることを明確にすることを希望します。

以上を前提に、両当事者は以下に同意します。

1. *データ共有活動*

本契約に関連して処理される個人データに関して、共有の主題、性質、目的および期間、ならびにデータ主体のカテゴリーおよび個人情報のカテゴリーは、『データ処理の詳細』と題する本契約の別紙に明記されています。

1. *適用範囲*

本DSAの規定は、本作業明細書に別段の定めがある場合を除き、本契約に基づくすべての本作業明細書に適用されます。

1. *サプライヤーの義務*

サプライヤーは、本契約に関連して個人データを処理する場合、以下の各号を行うものとします。

* 1. サプライヤーは、データ保護法および本DSAに基づくサプライヤーの義務を遵守し、これらの義務を履行できない場合には、直ちに当社に通知し、不遵守を是正するために当社が必要と考えるあらゆる合理的かつ適切な措置を講じます。
	2. サプライヤーは、以下の場合を除き、本DSA及び本契約において指定されている方法のみで個人情報を処理する。
		1. サプライヤーがデータ主体の事前同意を得ている場合
		2. 特定の行政手続、規制手続、または司法手続に関連して、法的請求の定立、行使、または防御のために必要な場合
		3. データ主体または他の自然人の重大な利益を保護する必要がある場合
		4. 適用法に別段の定めがある場合。この場合、サプライヤーは、適用法で禁止されている場合を除き、その法的要件を当社に通知するものとします。また、開示が要求されるデータの性質および範囲が最小となるように最善の努力を払い、適用法を遵守するために必要最小限の範囲でのみ個人データを開示するものとします。
	3. サプライヤーは、第三者に対し個人データを開示または移転してはならないものとします。ただし、当該第三者が本DSAおよび本契約に規定されているものと少なくとも同程度の個人情報保護義務を負う条件で、書面による契約を締結している場合には、この限りではありません。
	4. サプライヤーは、本契約に規定されている場合または本DSAにより別途許可されている場合を除き、本サービスを提供する目的以外で、個人データを販売、共有、保持、使用、または開示してはならないものとします。サプライヤーは、個人データへのアクセス権を有するサプライヤーの担当者について、（i）本サービスを実行するために個人データへのアクセスが必要であること、（ii）本DSAで許可された場合にのみ個人データを処理すること、および（iii）本DSAおよび本契約に基づくサプライヤーの義務と少なくとも同等の個人データ保護義務に服することを確実にするものとします。
	5. サプライヤーは、その社員、関連会社、代理人、下請業者、その他サプライヤーに代わる者のすべての行為または不作為について全面的に責任を負うものとします。
	6. サプライヤーは、合理的かつ適切な、書面による情報セキュリティプログラムおよびプライバシープログラムを導入し、維持するものとします。当該プログラムには、本契約において処理される個人データの性質に応じた、業界の優れた慣行（または別紙1で要求されるさらに高い基準）を満たすかこれを上回り、個人データを漏えい等から合理的に保護する物理的、技術的および組織的対策を組み込むものとします。これには、本DSAの要件を十分満たした方法で個人データ処理を行う責任を有するすべての担当者のトレーニング、別紙1に記載されている対策が含まれます。さらに、別紙1に記載のない範囲において、必要に応じて以下も含まれます。
		1. 個人データの仮名化および暗号化
		2. 処理システムおよびサービスの機密性、完全性、可用性、およびレジリエンスを継続的に確保する能力
		3. 物理的または技術的なインシデントが発生した場合に、個人データへのアクセスおよびその可用性を適時に回復する能力
		4. 処理のセキュリティを確保するための技術的および組織的対策の有効性を定期的にテスト、検証、評価するプロセス
		5. ある事象が個人データ漏えい等に該当するかどうかを検出後72時間以内に確認する能力
	7. サプライヤーは、自らの管理下で、または自らの行為または不作為に起因して、個人データの漏えい等が実際に発生した場合または発生したことが合理的に疑われる場合（以下「サプライヤーの個人データ漏えい等」といいます。）、以下のことを行うものとします。
		1. サプライヤーは、不当な遅滞なく、いかなる場合でも、サプライヤーの個人データ漏えい等が発覚してから24時間以内に当社に通知します。
		2. サプライヤーは、当社が満足する方法で、かかるサプライヤーの個人データ漏えい等を修正し、再発を防止するために必要な適切な調査およびあらゆる改善努力を実施します。
		3. サプライヤーは、記録の保持に関する情報および報告、その他サプライヤーの個人データ漏えい等に関して当社が合理的に要求するすべての情報を含め、当社がデータ保護法を遵守するために必要と考えるすべての情報を速やかに当社に提供します。
		4. サプライヤーは、その個人データが影響を受けた可能性のあるすべてのデータ主体に、データ保護法で要求される内容を記載した通知を提供するものとします。
		5. サプライヤーは、データ主体への通知をサプライヤーまたは当社のいずれが行ったかにかかわらず、いずれかの当事者が負担したかかる通知の費用および経費について単独で責任を負うものとします。
	8. サプライヤーは、以下のいずれかが発生した場合、これらの事項について、不当な遅滞なく速やかに、いかなる場合であっても24時間以内に、当社に通知するものとします。
		1. 本契約に関連する個人データに関する、管轄のデータ保護当局またはその他の規制当局から苦情、問い合わせ、要求または懸念の表明を受けた場合。
		2. 本契約に関連してサプライヤーが処理する個人データに関する、データ主体からの苦情、問い合わせ、要求、または懸念の表明を受けた場合。これには、個人データへのアクセス（個人データの処理に関する情報の要求も含みます）、修正、訂正、共有、削除、または処理の停止等の、データ保護法あるいは当社またはサプライヤーのプライバシーポリシーに基づく権利行使としての要求を含みます。
	9. サプライヤーは、サプライヤーおよび当社が、データ保護法および本DSAに基づくそれぞれの義務を遵守するために必要な、当社が要求するすべての合理的かつ適切な措置を実施するものとします。
	10. サプライヤーは、適用法において別途必要である場合を除き、データ共有目的を達成するために必要な期間を超えて個人データを保持しないものとします。サプライヤーは、当社から要請があった場合、ならびに本契約または個人データの処理について記載された作業明細書が満了または早期終了した場合、適用法に別段の定めがない限り、当社の判断に応じて、処理していたすべての個人データを速やかに削除または返却するものとします。その場合、サプライヤーは、適用法に基づいて保持が義務付けられている個人データの保存期間が終了してから30日後までの間、当該個人データのコピーを1部保持することができるものとし、かつ、保持する個人データに関しては、引き続き本DSAを遵守し、当該適用法で求められる個人データの処理のみを行うものとします。サプライヤーは、当社が合理的に要求する方法で、かつ、個人データを返却する場合には当社が合理的に要求する形式で、個人データを削除または返却するものとします。
	11. サプライヤーは、当社から共有を受けた個人データの正確性および完全性を、サプライヤーがかかる個人データを受領したのと同一の形式のまま、維持するものとします。
	12. サプライヤーは、個人データが、適用のある通知、同意、認可、および権利に従って、本DSAで許可されたとおりに処理されたこと、ならびに当社およびサプライヤーがデータ保護法を遵守して個人でデータを処理したことを証明できるようにするために必要なすべての記録を維持するものとします。
	13. サプライヤーは、当社の要請に応じて、サプライヤーの本DSAの遵守、ならびにサプライヤーのプライバシープログラムおよび情報セキュリティプログラムについて、当社または当社が義務付けた監査人による監査を許可し、これに協力するものとし、また第三者の監査人にサプライヤーのプライバシープログラムおよび情報セキュリティプログラムの監査を実施させるものとします。かかる監査は、データ保護法によって要求される監査、評価、またはレビューを妨げるような制限を除き、本契約に詳述されている合理的に適用可能な監査の制限および要件に従うものとします。
	14. サプライヤーは、個人データの国境を越えた移転に制限がある国または地域のデータ主体に関する個人データを処理する場合、必ずデータ保護法を遵守してこれを行うものとし、これには、個人データの移転を保護することを目的とした標準契約条項や同様の仕組みの締結が含まれます。
	15. サプライヤーは、より高い業界標準またはデータ保護法に適合するための変更を除き、本契約に関連して当社が直近実施したデューデリジェンスにおいてサプライヤーが当社に開示した、プライバシーおよびデータセキュリティの慣行を有効に維持し、その適用を継続するものとします。ただし、サプライヤーは、以前に開示した慣行を引き下げるようなプライバシーおよびデータセキュリティの慣行を後から開示することによって、慣行の基準を引き下げることはできません。サプライヤーは、かかるデューデリジェンスにおいて提供したすべての回答が、作成された時点で真実、正確、かつ完全であること、およびサプライヤーの正式な代表者がかかるデューデリジェンスを完了したことを表明し、保証するものとします。サプライヤーは、プライバシーおよびデータセキュリティの慣行に重大な変更があった場合、これを直ちに当社に通知するものとします。
	16. サプライヤーは、データ保護法により要求される場合、個人データ保護の担当者を任命し、その者の氏名および電話番号を当社に通知するものとします。
	17. サプライヤーは、本DSAの締結が、本DSAに定められた制約を理解し、遵守することを証明するものであることを認め、同意するものとします。
1. *補償*

両当事者は、サプライヤーが、当社およびその関連会社ならびにそれぞれの役員、取締役、社員、請負業者、派遣社員、下請業者、代理人、その他当社または関連会社に代わる者（以下それぞれを「被補償当事者」といいます。）に対し、サプライヤーが本契約に関連して処理した個人データに関連する個人データ漏えい等に起因して被補償当事者が被った損失、損害、罰金、費用、または経費（訴訟費用および支出を含みます。）について補償することに、当社の権利または権限、もしくは本契約に基づく義務またはその他の義務を制限することなく、同意するものとします。本条項に基づく責任については、かかる責任がサプライヤーの過失または故意の不法行為の結果生じた場合を除き、本契約における責任を制限または除外する規定の適用対象となるものとします。

1. *定義*
	1. 「データ保護法」とは、適用されるデータ保護法、データセキュリティ法、またはプライバシー法を意味します。これには、EU一般データ保護規則およびそれに関連する各国の施行法、医療保険の相互運用性と説明責任に関する法律（Health Insurance Portability and Accountability Act）、カリフォルニア州プライバシー権法（California Privacy Rights Act）、およびその他の国家、州、連邦、地方、または地域のデータ保護法、データセキュリティ法、またはプライバシー法を含みます。
	2. 「個人データ」とは、識別された個人または識別可能な個人の本契約に関連するあらゆる情報を意味し、個人を特定するデータ、および個人を識別、その位置を特定、追跡、連絡に使用できるデータを含みます。個人データには、名前、識別番号、固有の役職などの個人を直接識別可能な情報および生年月日、固有のモバイル端末またはウェアラブル端末の識別子、世帯を識別するために使用可能な情報、電話番号、キーコード化されたデータ、IPアドレスなどのオンライン識別子、または個人の活動、行動、嗜好などの間接的に個人を識別可能な情報の両方が含まれ、さらには、データ保護法において「個人データ」として規定されるあらゆるデータが含まれます。
	3. 「処理」とは、自動的な手段によるか否かを問わず、収集、記録、整理、構造化、保管、アクセス、修正または変更、検索、参照、使用、送信による開示、配布、またはその他の方法で利用可能にすること、評価、分析、報告、共有、整列または結合、制限、消去、破壊などのような、個人データもしくは一群の個人データに実施される操作又は一連の操作を意味します。
	4. 「個人データ漏えい等」とは、送信、保存、またはその他の方法で処理された個人データに対する偶発的または違法な破壊、紛失、改ざん、開示、使用、またはアクセスを意味します。
	5. 「標準契約条項」とは、欧州委員会が2021年6月4日に公表した、十分なレベルの保護を確保していない第三国への個人データの移転についての標準契約条項を意味し、随時更新される可能性があります。
	6. これらの定義に関して、データ保護法上より広い定義がとられている場合、本定義はデータ保護法上の定義と一致するように拡大して解釈されるものとします。
	7. 本項に定義がない場合、用語は、適用されるすべてのデータ保護法に準拠して解釈されるものとします。
2. *解釈*
	1. 本DSAで使用されているが、本DSAにおいて定義されていない定義語は、本契約中において定義された意味を有するものとします。
	2. 「含む」という言葉は、制限なく含むという意味に解釈されるものとします。
	3. サービス契約および本DSAに基づく義務を履行するにあたり、両当事者は、MSDおよびその関連会社の企業ポリシーが、EU一般データ保護規則を含む適用されるデータ保護法の文字および精神に基づいて、MSDのビジネスが行われることを要求していることを認識しています。 両当事者が同じデータ保護法の対象とならない場合、両当事者がそのような法律に含まれるすべての合理的に関連するデータ保護基準を遵守することが期待されています。
	4. 本契約に基づく本データ共有目的に関連して、サプライヤーは当社の関連会社の個人データを処理することがあります。かかる場合には、当該当社関連会社は、個人情報の「管理者」および本DSAの第三者受益者とみなされ、当該当社関連会社が本契約または本DSAの当事者として指定されているかどうかにかかわらず、本DSAに基づいて当社に与えられるすべての権利および保護に依拠し、行使する権利を有するものとします。
	5. 本DSAは、本契約に組み込まれ、一体として一つの契約を構成します。
	6. 本契約の条件と本DSAの条件が矛盾する場合、その矛盾する範囲においては、本DSAの条件が優先されます。ただし、本契約の条件が本契約に関連して処理される個人データに関してより保護的な定めをおいている場合を除き、かかる場合には、本契約のより保護的な条件が優先されるものとします。
	7. 本DSAの条件と標準契約条項との間に矛盾がある場合、その矛盾する範囲においては、標準契約条項の条件が優先されるものとします。
	8. 本契約の規定は、本DSAにおいて明示的に修正された場合を除き、引き続き完全な効力を有します。
	9. 本DSAが英語およびそれ以外の言語で作成されている場合に、これらの内容に相違があるときには、英語で作成された本DSAの内容が優先されるものとします。
	10. 本DSAの見出しは、参照時の便宜のために記載したものであり、本DSAの一部を構成するものではなく、また本DSAの意味や解釈に影響を与えるものでもありません。
	11. 本DSAの別紙および添付資料は、本DSAと不可分一体をなすものであり、本DSAにそのまま記載されているのと同様に扱います。
	12. 本DSAの規定は分離可能です。いずれかの文言、条項、規定の全体または一部が無効であるか、または法的強制力がないとしても、その他の文言、条項、または規定の有効性または法的拘束力に影響を与えるものではなく、本DSAのその余の部分は完全な効力を有するものとします。
	13. 本DSAは、当社とサプライヤーが、本データ共有目的に適用される別のDSAを締結している場合を除き、本契約を補足するものとして、本データ共有目的に関連する個人データの処理に適用されます。
	14. 本DSAは、複数の副本によって締結することができ、各副本はいずれも正本とみなされ有効であり、すべて一体として単一かつ同一の契約を構成します。いずれの当事者も、当該副本を締結することにより、本DSAを締結することができます。
	15. 本DSAは、本DSAの主題に関する両当事者間の完全な合意を構成し、（法律上許容される限りにおいて）当該主題に関する両当事者間のすべての事前の表明または口頭もしくは書面による合意に優先するものとします。ただし、本DSAのいかなる規定も、また、いずれの当事者も、虚偽の陳述に対する責任を免れるものではありません。
	16. 本DSAには、本契約の準拠法および管轄規定が適用されます。
3. *アップデートの制限*
	1. 当事者が契約を更新、修正、契約の下で新たな作業指示書を発行、または契約または契約の下での任意の作業指示書をいかなる方法で変更する場合（「引き金となるイベント」）、<https://www.msdprivacy.com/privacyterms/> に位置する「Data Sharing Addendum (Company Data)」のもとでの最新の文書が、次の引き金となるイベントまでこのDSAの条項を上書きし、置き換えることになりますが、引き金となるイベントの発生後30日以内に異議が唱えられない限りです。それにもかかわらず、新しい適用可能なデータ保護法、判例、または関連するデータ保護当局によって発行されたガイダンスに準拠するために必要なものに限定された新しいまたは修正された条項を確保した後に、誠実にのみ行われるべきであり、本DSAの条項に即時の修正が必要とされる状況が存在する可能性があります。これは7(b)で述べられた理由によりのみ発生します。
	2. 次のいずれかのシナリオが発生した場合、当事者は直ちに上記のアドレスで掲載されている最新の条項に同意することになりますが、これはprivacy\_updates@msd.comで通知を受け取ることを要求したすべての実体に対して新しい条項を通知した後の30日以内に異議が唱えられない限りです。

		1. 適用されるデータ保護法が更新され、このDSAの既存の契約条項が更新された法律の要件を満たすには不十分である場合、
		2. 適用されるデータ保護法に変更があり、当事者が法律の変更によりこれらの条項を修正する合理的かつ正当な利益を持っている場合、例えば制約なく、もはや必要ではない要件を削除する場合など、

新しい判例または関連するデータ保護当局によって発行されたガイダンスがあり、その効果が上記(i)または(ii)で説明された法律の変更と同等である場合。

1. *別紙の適用範囲*

別紙2として本書に添付されている標準契約条項および別紙3として添付されている追加条項は、適用されるデータ保護法で要求される範囲においてのみ適用されるものとします。両当事者は、それぞれの法域において適用されるデータ保護法の要件と一致し、その要件によって必要とされる場合に限り、かかる条項および追加条項を遵守することに同意します。

1. *通知*

本DSAに基づいて行われる通知（以下「通知」といいます。）は、書面で行われるものとします。本DSAに基づいて行われる通知は、本契約の通知に関する規定に従って行われるものとし、当社宛（msd\_privacy\_office@msd.com）に電子メールでコピーを送信するものとします。件名は「DSA Notice from Supplier（サプライヤーからのDSAに関する通知）」、または個人データ漏えい等の場合は「Urgent:Personal Data Breach Notice（緊急：個人データ漏えい等に関する通知）」とするものとします。

**別紙1 – 情報技術セキュリティ対策**

1. **定義－**本別紙で使用されている場合、以下の各定義語は、当該用語について以下に定める定義を有する。本別紙で使用されているが、本別紙で定義されていない定義語は、主契約または本覚書のいずれかの条項に定める意味を有するものとする。
	1. 「甲情報」とは、本サービスに関連して乙または乙の第三者サービスプロバイダに提供された、またはこれらによって取得、作成、もしくは生成された、またはその他の方法で処理された、甲または甲の関連会社もしくはその乙、顧客、その他の取引先の情報、および主契約または本覚書に基づき秘密として扱われるべきその他の情報をいう。
	2. 「データ侵害」とは、甲情報の偶発的もしくは不正な破壊、紛失、変更、使用、送信、もしくは開示、または甲情報へのアクセスをいう。
	3. 「エンドポイント」とは、外部の第三者サイト（クラウドプロバイダなど）でホストされているものを含め、乙システム上のラップトップもしくはデスクトップ、モバイルデバイス、ラボ機器、サーバー、またはその他のデバイスを含む、すべてのコンピューターをいう。
	4. 「通知イベント」とは、法律に基づき個人または事業体への通知を必要とするすべてのイベント（データ侵害を含む）をいう。
	5. 「セキュリティイベント」とは、（A）データ侵害、（B）通知イベント、（C）乙システムの運用に対する不正なアクセスもしくは妨害、または（D）本別紙、主契約もしくは本覚書、もしくは法律に基づく乙のセキュリティ義務違反をいう。
	6. 「対象ソフトウェア」とは、本サービスに関連して提供または使用されるソフトウェアをいう。これには、甲もしくは甲の関連会社の、またはこれらの情報システムに接続された、コンピューター（ラップトップもしくはデスクトップ、モバイルデバイス、ラボ機器、サーバー、その他のデバイスもしくはコンポーネントを含む）に配信もしくはインストールされているすべてのソフトウェアが含まれる。
	7. 「乙システム」とは、以下の対象ソフトウェアを含む、乙のネットワークおよびすべてのシステムをいう。（A）本サービスに関連して提供または使用されるもの、（B）甲情報または甲もしくはその関連会社向けの成果物もしくは仕掛品が保存される、もしくはその他の方法で処理される、またはこれらへアクセスができるもの、（C）甲もしくはその関連会社の情報、ネットワーク、もしくはその他のシステムに接続されている、または甲もしくはその関連会社の情報、ネットワーク、もしくはその他のシステムへのアクセスを可能にするもの、または（D）上記のいずれかを接続することができる、または上記のいずれかへのアクセスを可能にするもの。

1. **ネットワークセキュリティ－**乙は、乙の業界のベストプラクティスに従って、ネットワークセキュリティポリシー、手順、および規制を維持し、ネットワークセキュリティ活動を実施するものとする。ただし、それには少なくとも、乙の業界のベストプラクティスに従って定期的に（ただし、少なくとも年に一度）実施するネットワークファイアウォールプロビジョニング、侵入検知および予防の制御、分散型サービス拒否（DDoS）攻撃防御管理、ならびに脆弱性評価および侵入テストが含まれる。いかなる場合も、甲情報および乙システムの保護に適用される乙ネットワークセキュリティポリシー、手順、または規制は、乙が自らの情報および同様の性質を有するその他のシステムの保護に適用するものと同程度に厳格で保護的なものとする。
2. **アプリケーションセキュリティ－**提供するサービスの性質に基づき、該当する場合、乙は、乙ソフトウェアの開発および変更（アップデート、アップグレード、パッチ、機能強化、バグ修正、修正、改良、訂正、改訂、リリース、その他の変更を含む）を管理するソフトウェア開発ライフサイクルプロセスと制御（以下「SDLCプロセス」という）を備えるものとする。SDLCプロセスには、少なくとも、承認された同等の業界標準のセキュアソフトウェア開発プラクティスが含まれるものとする。乙は、乙情報システムが適切なセキュリティと機能を備えた最新版であることを確保するパッチ管理プロセスに従うものとする。乙は、適時に、リスクに応じて、乙ポリシーおよび手順に定められた期限内に、特定された脆弱性を是正し、再試験を行うものとする。
3. **データセキュリティ－**提供するサービスの性質に基づき、該当する場合、乙は、第11項に定めるような承認された同等の業界慣行と標準（該当する場合、PCI DSSを含む）に従い、かつすべての法律に従い、甲情報の取り扱い、保存、およびその他の方法での処理を行うものとする。乙は、データ侵害に対して合理的な予防措置を確立し、維持するものとする。乙の他の義務に加え、また、それらを制限することなく、乙は、乙の業界のベストプラクティスに従い、かつすべての法律を遵守して、すべての甲情報を保存するものとし、乙の業界のベストプラクティスを満たすセキュリティ対策（暗号化やファイアウォールを含む）を用いて、データ侵害から甲情報を保護するものとする。乙が甲情報をオフサイト施設に保管する場合、乙は、主契約もしくは本覚書、または第三者への甲情報の開示、もしくは製品やサービスの提供、もしくはその提供支援のための第三者の雇用について主契約もしくは本覚書に関連して締結された契約の、すべての条件を遵守していなければならない。また、乙は、上記を制限することなく、本別紙のすべての規定に完全に準拠した、甲が合理的に受け入れられるオフサイト保管施設を使用するものとする。さらに、当該オフサイト保管施設の提供者は、乙と当該提供者との間の書面による秘密保持契約の拘束を受けなければならない。秘密保持契約は、主契約もしくは本覚書またはこれらに関連して締結された契約の条件と同程度に厳格な条件を含み、かつ、そこに記載されているすべての甲情報を保護するものでなければならない。
4. **データストレージ－**提供するサービスの性質に基づき、該当する場合、あらゆる甲情報の取り扱い、保存、およびその他の方法での処理は、指定された乙のコンピューティング・リソースおよびストレージ・リソース上でのみ行われる。甲情報は、以下の場合、ラップトップまたはモバイルデバイス上でのみ取り扱われ、保存され、もしくはその他の方法で処理され、またはこれらに転送される。（A）乙のラップトップまたはモバイルデバイスである場合、（B）乙が、下記第7項の暗号化基準に従い、当該ラップトップまたはモバイルデバイス上のすべての甲情報を暗号化する場合、および（C）当該ラップトップまたはモバイルデバイスが、第11項に定めるような承認された同等の業界慣行と標準に準拠したエンドポイント制御の対象である場合。甲情報は、上記の文に規定されている場合を除き、ポータブルデバイス上での取り扱い、保管、またはその他の方法での処理を行わない。乙は、指定されたバックアップおよびリカバリプロセスの一環として甲情報のすべてのバックアップを保存するものとし、甲情報の当該バックアップは、本別紙（本第5項および下記第7項の要件を含む）に従って暗号化しなければならない。
5. **データ送信－**提供するサービスの性質に基づき、該当する場合、甲情報の電子送信または交換は、第11項に定めるような承認された同等の業界慣行と標準に準拠し、かつ下記第7項にのみ従い、確実な手段（HTTPSもしくはSFTPまたはこれらと同等のものの使用）によって行うものとする。
6. **データ暗号化－**提供するサービスの性質に基づき、該当する場合、乙の他の義務に加え、また、それらを制限することなく、乙は、法律に基づき保護の対象となる個人情報で構成される、もしくはその時点で最新のペイメントカード業界データ保護基準に基づき保護の対象となる情報で構成される、すべての甲情報（甲のすべてのバックアップデータを含む）を、商用サポートされた暗号化ソリューションを用いて暗号化された形式で保存するものとすることに同意する。乙は、第11項に定めるような承認された同等の業界慣行と標準に従って、甲情報を暗号化する暗号化ソリューションを展開するものとすることに同意する。ただし、対称暗号化の場合は128ビット以上のキー長、非対称暗号化の場合は2048ビット（またはそれ以上）のキー長を使用する。
7. **データの再利用－**提供するサービスの性質に基づき、該当する場合、乙は、本サービスの履行のみを目的として、あらゆる甲情報を使用するものとする。乙は、乙の他のアプリケーション、環境、もしくは事業部門に、甲情報を配布、転用、または共有しないものとする。
8. **契約終了時のデータの取り扱い－**提供するサービスの性質に基づき、該当する場合、乙の他の義務に加え、また、それらを制限することなく、甲の要求に応じて、主契約もしくは本覚書に別段の定めがある場合を除き、主契約の満了時または早期終了時に、乙または乙の関連会社、下請業者、サービスプロバイダ、代理店、その他のコンサルタントが所有または管理しているすべての甲情報を甲が選択した方法により破棄または返却するものとする。
9. **セキュリティ侵害の通知－**乙の他の義務に加え、また、それらを制限することなく、乙は、実際のまたは合理的に疑われるセキュリティイベントを認識してから24時間以内に、当該実際のまたは合理的に疑われるセキュリティイベントを甲に通知するものとする。乙は、当該実際のまたは合理的に疑われるセキュリティイベントについて、電話（+1-704-345-6700－オプション1を選択する）および電子メール（グローバルオペレーションセンター：globalopscnt@merck.com; globaloperationscentertier3@merck.com; goc@merck.com ）により甲のセキュリティチームに連絡することで甲に通知するものとする。乙は、セキュリティイベントについて甲が合理的に要求することができる情報および支援（根本原因情報を含む）を提供する。
10. **業界標準－**一般に認められている業界標準には、以下により定められ維持されている現行の基準やベンチマークが含まれるが、これらに限定されない。
	1. インターネットセキュリティセンター－[https://www.cisecurity.org](https://www.cisecurity.org/)を参照
	2. ペイメントカード業界／データセキュリティ基準（PCI/DSS）－
	 <https://www.pcisecuritystandards.org/>を参照
	3. 米国国立標準技術研究所－[https://csrc.nist.gov](https://csrc.nist.gov/)を参照
	4. 連邦情報セキュリティ管理法（FISMA）－[https://csrc.nist.gov](https://csrc.nist.gov/)を参照
	5. ISO/IEC 27000シリーズ－<https://www.iso27001security.com/>を参照
	6. 構造化情報標準促進協会（OASIS）－<https://www.oasis-open.org/>を参照
	7. オープンウェブアプリケーションセキュリティプロジェクト（OWASP）－[https://www.owasp.org](https://www.owasp.org/)を参照
	8. CWE（共通脆弱性タイプ一覧）－[https://cwe.mitre.org](https://cwe.mitre.org/)、またはCWE/SANS最も危険なプログラミングエラーTop 25－<https://cwe.mitre.org/top25/>を参照
	9. SANSインスティテュート－[https://www.sans.org](https://www.sans.org/)を参照
	10. 最も危険なソフトウェアエラー－<https://www.sans.org/top25-programming-errors/>を参照

甲の合理的な要求に応じて、乙は、甲が乙による上記の要件の遵守を監査することを許可するものとする。乙は、要件の不遵守があった場合には、合理的に可能な限り速やかに是正するものとする。

**別紙2**

当社が標準契約条項のモジュール2の適用となる方法で個人情報を輸出する場合には、以下の条件が適用されます。

*2021年6月4日付欧州委員会実施決定（EU）2021/914に添付された標準契約条項のモジュール1（管理者から管理者への移転）の本文は、参照により、ここに組み込まれるものとします。オプションについては以下で説明します。*

1. *第7条（ドッキング条項）は省略されます。*
2. *第11条に関して、選択的な条項が省略されます。*
3. *第17条に関して、加盟国がオランダであるオプション1が選択されます。*
4. *第18条に関して、法廷地としてオランダが選択されます。*

**別紙2の添付資料1**

**A. 当事者リスト**

*本契約を参照*

**B. 移転の説明**

*『データ処理の詳細』と題する本契約の別紙を参照*

**C. 管轄権を有する監督機関**

****Commission Nationale de l'Informatique et des Libertés - CNIL****
3 Place de Fontenoy

TSA 80715

75334 PARIS CEDEX 07
Tel. +33 1 53 73 22 22
Fax +33 1 53 73 22 00
Website: [**http://www.cnil.fr/**](http://www.cnil.fr/)

**別紙2の添付資料2 – 技術的および組織的対策**

これらの条項が添付されている本DSA別紙1を参照してください。さらに、データ輸入者は、すべての個人データが必要に応じて仮名化され、暗号化されていることを保証するものとします。また、データ輸入者およびその関連会社は、本条項の対象となる個人データに関連する要請を政府当局から受けた場合、別紙2添付資料1のBに記載されている個人データの（i）米国またはその他の国や地域の諜報機関またはこれに類する当局からのアクセスの要求、および（ii）開示義務について、データ輸入者およびその関連会社が、個人データを抽出する前に、適用される法規制に従って異議を申し立てることを保証します。

**別紙3**

**その他の州、国、地域、および地方の法的要件**

**英国に関する追加条項：2018年データ保護法**

本別紙3には、2022年3月21日発効の欧州委員会標準契約条項の国際データ移転追加条項バージョンB1.0が参照により組み込まれており、本DSAにおける適用可能な移転のすべてがカバーされ、同追加条項のパート2（必須条項）全体を含むすべてが、本契約のすべての当事者によって合意されたものとみなされます。

**スイスに関する追加条項：FADP**

1. 別紙2に記載されているデータ移転がFADPの対象である限り、GDPRへの言及はスイス連邦データ保護法（「FADP」）へ言及しているものと解釈します。
2. FADPで要求されている限り、法人の個人データは、個人がデータ主体である場合と同様に、以下の条項に従って保護されるものとします。
3. 第13条：並行監視
	1. データ移転がFADPによって管理される場合：連邦データ保護情報コミッショナー（「FDPIC」）が、管轄権を有する監督機関です。
	2. データ移転がGDPRによって管理される場合：第13条（a）の基準が適用されるものとします。
4. 第18条（c）：法廷地および管轄の選択：スイスに常居所を有するデータ主体は、データ輸出者および／またはデータ輸入者に対して、スイスの裁判所で法的手続きを取ることができます。

**カナダに関する追加条項：ケベック州法25**

* + - 1. 個人データ漏えい等に関連して本DSAに基づいて要求される通知、および本契約に基づいて要求される同様の通知は、サプライヤーが本DSAに違反した際、または違反しようとした際にも要求されるものとします。
			2. 本DSAの条件に関連して同意を収集する必要がある場合、サプライヤーは本契約の終了後3年間、すべての同意について、その証拠を保持しなければなりません。

**アラブ首長国連邦付加条項: 個人データ保護に関する連邦法第45号（2021年）**

1. 付録2で記載されたデータ転送がアラブ首長国連邦の個人データ保護に関する連邦法第45号（2021年）（「PDPL」）の対象となる場合、アラブ首長国連邦のデータオフィスが個人情報をアラブ首長国連邦外に転送するための独自の標準契約条項を発行し、両当事者がそのような標準契約条項を締結するまで、両当事者は、付録2に添付された標準契約条項が、個人情報およびデータ主体の適切な保護措置を提供するために、そのような転送に関連して、mutatis mutandisの適用を受けることに同意します。この目的のために： a. 「EU一般データ保護規則（Regulation (EU) 2016/679）」、および「自然人の個人データの処理に関する2016年4月27日の欧州議会および理事会の規則（EU）2016/679（一般データ保護規則）」および「その規則」に関する言及はすべて「PDPL」に置き換えられます。 b. 「EU一般データ保護規則（Regulation (EU) 2016/679）」の特定の記事に関する言及は、「PDPL」の同等の記事またはセクションに置き換えられます。 c. 「欧州連合」、「連合」、「EU」、「EU加盟国」、「加盟国」、「EUまたは加盟国」に関する言及はすべて「アラブ首長国連邦」に置き換えられます。 d. 「適格な監督当局」および「監督当局」に関する言及は、すべて「データオフィス」に置き換えられます。 e. 標準契約条項に関するいかなる紛争も、アラブ首長国連邦の法律に従って解決され、アラブ首長国連邦の裁判所で解決されます。両当事者は、そのような裁判所の管轄権に従うことに同意します。 f. 付録2に添付された標準契約条項とPDPLの間に矛盾または対立がある場合、PDPLが適用されます。 g. 付録2に添付された標準契約条項の意味が不明確であり、アラブ首長国連邦外への個人情報の転送に適用される場合、または複数の意味がある場合は、PDPLに最も近い意味が適用されます。
2. アラブ首長国連邦のデータオフィスが、アラブ首長国連邦外への個人情報の転送を合法化するための独自の標準契約条項を発行する場合、両当事者は誠意を持って交渉し、合理的に実行可能な最も早い時期に標準契約条項を合意し、実施することを目指します。前文の文に従って両当事者が標準契約条項を締結した場合、PDPLの対象となるアラブ首長国連邦外への個人情報の転送に関して、付録2に添付された標準契約条項が、転送に関連して個人情報およびデータ主体の適切な保護措置を提供するために実施された適切な保護措置として置き換えられます。
3. データオフィスが標準契約条項が適用される個人情報の転送を対象とする適格決定を採択した場合、または会社がその他の適切な保護措置が転送に関連して適用されると判断した場合、会社は、付録2に添付された標準契約条項に拘束される合意を、サプライヤーに書面で通知することによって取り消すことができます。前文に従って会社が発した通知の日付から、付録2に添付された標準契約条項は、アラブ首長国連邦外のPDPLの対象となる個人情報の転送に適用されなくなります。

**ブラジル付属書: LGPD - 標準契約条項**

一般データ保護法（Lei Geral de Proteção de Dados –「LGPD」）に基づくブラジルの標準契約条項（「SCCs」）は、ブラジルの居住者のデータが処理される場合、またはデータ移転がそれらの適用を必要とする場合に遵守されなければなりません。 当事者は、ブラジル国家データ保護機関（「ANPD」）によって発行された通りにSCCsを完全に採用することに同意し、条項で明示的に許可された条件に従って修正されない限り、これを適用します。これらのSCCsは、本契約に参照として組み込まれ、複数のテキストオプションが提示されている場合には次の選択が行われます。

セクション3.1にはオプションBが選択されます。インポーターは、以下に記載されている条件およびCLAUSE18の規定に従い、これらの条項に基づく国際データ移転の対象となる個人データの転送を行うことができます。

セクション4.1にはオプションAが選択されます。 相互支援義務と当事者の一般義務を損なうことなく、以下の指定当事者が、これらの条項で規定されている義務を主に遵守する責任を負います：

a) CLAUSE14で提供される文書の発行責任者：

[x] エクスポーター [ ] インポーター

b) CLAUSE15で処理されるデータ主体からの要求への対応責任者：

[x] エクスポーター [ ] インポーター

c) CLAUSE16で提供されるセキュリティインシデントの通知責任者：

[x] エクスポーター [ ] インポーター

**サウジアラビア付属書: PDPL - 標準契約条項**

個人データ保護法（「PDPL」）に基づくサウジアラビアの標準契約条項（「SCCs」）は、サウジアラビアの居住者のデータが処理される場合、データ移転がサウジアラビアの管轄に属する場合、またはサウジアラビアの法律がサウジのSCCsの遵守を要求する場合に組み込まれます。 附属書2で説明されたテンプレートタイプと一致するSCCsバージョンが完全に適用され、本契約に参照として組み込まれています。