**ANEXO DE INTERCAMBIO DE DATOS (DATOS DE LA COMPAÑÍA)**

**Fecha de revisión: 12 de marzo de 2024**

A los efectos de este Anexo de Intercambio de datos (Data Sharing Addendum, “DSA”), la entidad o afiliada de Merck Sharp & Dohme LLC que celebra el contrato u otra forma de acuerdo que hace referencia a este DSA (el “Acuerdo”) se denominará “Compañía” y todas las otras partes de dicho Acuerdo se denominarán colectivamente “Proveedor”. La Compañía y el Proveedor son cada uno una “Parte” y, en conjunto, las “Partes”.

Información general

1. Las Partes celebraron el Acuerdo, y junto con el Acuerdo pueden celebrar órdenes de compra o de trabajo, acuerdos de proyecto, anexos al plan de proyecto, declaraciones de trabajo, órdenes de trabajo u otros términos de servicio (cada uno una “Declaración de trabajo”), que rigen los servicios allí contemplados (el “Propósito del intercambio de datos”).
2. Las Partes desean complementar los términos del Acuerdo para garantizar que todo el intercambio de Información personal en relación con el Acuerdo se realice de conformidad con la Ley de Protección de Datos y para aclarar la función del Proveedor como controlador independiente de dichos datos.

Las Partes acuerdan lo siguiente:

1. *Actividades de Intercambio de datos*. En relación con la Información personal Procesada en relación con el Acuerdo, el objeto, la naturaleza, el propósito y la duración del Intercambio, las categorías de Sujetos de datos en cuestión y las categorías de Información personal se especifican en el anexo del Acuerdo titulado “Detalles de Procesamiento de datos”.
2. *Aplicabilidad*. Los términos de este DSA se aplican a cada Declaración de trabajo bajo el Acuerdo a menos que se especifique lo contrario en esa Declaración de trabajo.
3. *Obligaciones del Proveedor*. Al Procesar Información personal en relación con el Acuerdo, el Proveedor deberá:
   1. Cumplir con la Ley de Protección de Datos y las obligaciones del Proveedor en virtud de este DSA, y en caso de que el Proveedor no pueda cumplir con estas obligaciones, el Proveedor deberá notificar a la Compañía de inmediato y tomar todas las acciones razonables y apropiadas que la Compañía considere necesarias para remediar el incumplimiento.
   2. Procesar Información personal únicamente según lo especificado en este DSA y el Acuerdo, excepto en los siguientes casos:
      1. El Proveedor obtuvo el consentimiento previo del sujeto de datos.
      2. Es necesario para el establecimiento, el ejercicio o la defensa de reclamaciones legales en el contexto de procedimientos administrativos, regulatorios o judiciales específicos.
      3. Es necesario para proteger intereses vitales del sujeto de datos o de otra persona física.
      4. La ley aplicable exige lo contrario, en cuyo caso, el Proveedor deberá informar a la Compañía de ese requisito legal, a menos que lo prohíba la ley aplicable y hará todo lo posible para limitar la naturaleza y el alcance de cualquier divulgación requerida y solo divulgará la cantidad mínima de Información personal necesaria para cumplir con la ley aplicable.
   3. No divulgar ni transferir Información personal a ningún tercero sin que ese tercero celebre un acuerdo por escrito con términos que, como mínimo, protejan la Información personal como las obligaciones establecidas en este DSA y el Acuerdo.
   4. No vender, compartir, retener, usar o divulgar Información personal para otros fines que no sean los especificados en el Acuerdo o según lo autorizado en virtud de este DSA.
   5. Ser totalmente responsable de todos los actos o las omisiones de sus empleados, afiliadas, agentes, subcontratistas y otros representantes.
   6. Implementar y mantener programas escritos razonables y apropiados de seguridad y privacidad de la información, que incorporarán medidas físicas, técnicas y organizativas que sean proporcionales a la naturaleza de la Información personal Procesada en relación con el Acuerdo, que cumplan o superen las buenas prácticas de la industria (o estándares más altos que puedan requerirse en el Apéndice 1) y que protejan razonablemente contra un Incumplimiento de datos personales, incluida la capacitación de todo el personal responsable del Procesamiento de Información personal de manera suficiente para cumplir con los requisitos de este DSA, las medidas descritas en el Apéndice 1 y en la medida en que no se traten de otro modo en el Apéndice 1 y según corresponda:
      1. La seudonimización y el cifrado de la Información personal.
      2. La capacidad de garantizar la confidencialidad, la integridad, la disponibilidad y la resiliencia continuas de los sistemas y servicios de Procesamiento.
      3. La capacidad de restaurar la disponibilidad y el acceso a la Información personal de manera oportuna en caso de un incidente físico o técnico.
      4. Un proceso para probar, analizar y evaluar periódicamente la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del Procesamiento.
      5. La capacidad de confirmar dentro de las 72 horas posteriores a la detección si un evento constituye un Incumplimiento de datos personales.
   7. En caso de un Incumplimiento de datos personales real o razonablemente presunto de la Información personal dentro de la custodia o el control del Proveedor o que resulte de los actos o las omisiones del Proveedor (un “Incumplimiento de datos personales del Proveedor”), el Proveedor deberá:
      1. Notificar a la Compañía sin excesiva demora (y en cualquier caso dentro de las 24 horas posteriores a tener conocimiento de un Incumplimiento de datos personales del Proveedor).
      2. Llevar a cabo una investigación adecuada y todos los esfuerzos correctivos necesarios para rectificar y evitar que se repita dicho Incumplimiento de datos personales del Proveedor de manera satisfactoria para la Compañía.
      3. Proporcionar de inmediato a la Compañía toda la información que la Compañía considere necesaria para permitirle cumplir con la Ley de Protección de Datos, incluso con respecto al mantenimiento de registros e informes, y toda otra información que la Compañía pueda solicitar razonablemente con respecto a un Incumplimiento de datos personales del Proveedor.
      4. Proporcionar aviso a todos los Sujetos de datos cuya Información personal pueda haberse visto afectada, con el contenido requerido según la Ley de Protección de Datos.
      5. Asumir la responsabilidad exclusiva de los costos y los gastos de cualquiera de las Partes por dicho aviso a los Sujetos de datos, ya sea que el aviso haya sido realizado por el Proveedor o la Compañía.
   8. Notificar de inmediato a la Compañía sin demoras excesivas y en cualquier caso dentro de las 24 horas posteriores a lo siguiente:
      1. Cualquier queja, consulta, solicitud o inquietud por parte de una autoridad de protección de datos competente u otra autoridad reguladora relacionada con la Información personal vinculada con el Acuerdo.
      2. Cualquier queja, consulta, solicitud o inquietud de un Sujeto de datos relacionada con la Información personal vinculada con el Acuerdo, incluida cualquier solicitud para ejercer derechos según la Ley de Protección de Datos o la Política de Privacidad de la Compañía o del Proveedor, por ejemplo, acceder (incluido solicitar información sobre cualquier procesamiento de su Información personal), rectificar, modificar, corregir, compartir, eliminar o dejar de Procesar su Información personal.
   9. Cumplir con todas las medidas razonables y apropiadas solicitadas por la Compañía y necesarias para que el Proveedor y la Compañía cumplan con sus respectivas obligaciones en virtud de la Ley de Protección de Datos y este DSA.
   10. No retener la Información personal durante más tiempo del necesario para lograr el Propósito del intercambio de datos, a menos que la ley aplicable exija lo contrario.
   11. Mantener la exactitud y la integridad de la Información personal que comparte la Compañía, de acuerdo con el formulario en que el Proveedor recibió dicha Información personal.
   12. Mantener todos los registros necesarios para poder demostrar que la Información personal solo se Procesó de acuerdo con los avisos, los consentimientos, las autorizaciones y los derechos aplicables, y según lo permitido en virtud de este DSA y para que cada Compañía y Proveedor cumplan con la Ley de Protección de Datos.
   13. En la medida en que el Proveedor deba Procesar Información personal sobre Sujetos de datos de cualquier país o región con restricciones en la transferencia transfronteriza de Información personal, el Proveedor solo lo hará de conformidad con la Ley de Protección de Datos, que puede incluir la celebración de las Cláusulas contractuales estándar o mecanismos similares destinados a proteger las transferencias de Información personal.
   14. Excepto por los cambios realizados de conformidad con el cumplimiento de un estándar más alto de la industria o la Ley de Protección de Datos, el Proveedor mantendrá en vigor y aplicará de manera sistemática las prácticas de privacidad y seguridad de datos del Proveedor divulgadas a la Compañía en relación con cualquier diligencia debida que la Compañía haya realizado más recientemente sobre esas prácticas en relación con el Acuerdo; siempre que el Proveedor no pueda reducir los estándares en esas prácticas al divulgar posteriormente prácticas de privacidad y seguridad de datos que serían una degradación de las prácticas divulgadas anteriormente. El Proveedor declara y garantiza que todas las respuestas proporcionadas por el Proveedor en dicha diligencia debida son verdaderas, precisas y completas cuando se realizan, y que un representante autorizado del Proveedor completó dicha diligencia debida. El Proveedor deberá notificar de inmediato a la Compañía sobre todos los cambios importantes en las prácticas de privacidad y seguridad de datos del Proveedor.
   15. Si lo exige la Ley de Protección de Datos, designar a una persona a cargo de la protección de la Información personal e informar a la Compañía el nombre y el número de teléfono de la persona.
   16. El Proveedor reconoce y acepta que la firma de este DSA constituye su certificación de que comprende las restricciones establecidas en este DSA y que las cumplirá.
4. *Indemnización*. Sin limitar ninguno de los derechos de la Compañía, ni las obligaciones del Proveedor en virtud del Acuerdo o de otro modo, las Partes acuerdan que el Proveedor indemnizará a la Compañía y sus afiliadas, y sus respectivos funcionarios, directores, empleados, contratistas, trabajadores temporales, subcontratistas, agentes y otros representantes (cada uno una “Parte indemnizada”) por cualquier pérdida, daño, multa, costo o gasto (incluidos gastos y desembolsos legales) incurridos por esa Parte indemnizada como resultado de un Incumplimiento de datos personales del Proveedor en relación con la Información personal Procesada por el Proveedor en relación con el Acuerdo. Cualquier responsabilidad en virtud de esta sección estará sujeta a las limitaciones o las exclusiones de responsabilidad aplicables en el Acuerdo, a menos que dicha responsabilidad sea el resultado de la negligencia del Proveedor o un acto indebido intencional, en cuyo caso no se aplicarán limitaciones o exclusiones.
5. *Definiciones*
   1. “Ley de Protección de Datos” significa cualquier ley aplicable de protección de datos, seguridad de datos o privacidad, incluido el Reglamento General de Protección de Datos de la Unión Europea (UE) y cualquier legislación nacional de implementación relacionada con este, la Ley de Portabilidad y Responsabilidad de los Seguros Médicos, la Ley de Derechos de Privacidad de California y cualquier otra ley nacional, estatal, federal, provincial o regional de protección de datos, seguridad de datos o privacidad.
   2. “Información personal” significa cualquier dato vinculado con el Acuerdo relacionado con un individuo identificado o identificable, incluidos los datos que identifican a un individuo o que podrían usarse para identificar, localizar, rastrear o contactar a un individuo. La Información personal incluye tanto información de identificación directa, como un nombre, número de identificación o cargo único, como información de identificación indirecta, como fecha de nacimiento, identificador único de dispositivo móvil o portátil, información que podría usarse para identificar un hogar, número de teléfono, datos codificados con clave, identificadores en línea, como direcciones IP, o actividades, comportamientos o preferencias personales, e incluye cualquier dato que constituya “datos personales” según la Ley de Protección de Datos.
   3. “Procesar” significa realizar cualquier operación o conjunto de operaciones sobre Información personal o conjuntos de Información personal, ya sea por medios automatizados, tales como recopilación, registro, organización, estructuración, almacenamiento, acceso, adaptación o alteración, recuperación, consulta, uso, divulgación mediante transmisión, difusión o puesta a disposición de otro modo, evaluación, análisis, presentación de informes, intercambio, alineación o combinación, restricción, borrado o destrucción.
   4. “Incumplimiento de datos personales” significa una destrucción, pérdida, alteración, divulgación no autorizada o acceso accidental o ilegal a Información personal, transmitida, almacenada o Procesada de otra manera.
   5. “Cláusulas contractuales estándar” hace referencia a las cláusulas contractuales estándar para la transferencia de datos personales a países terceros, los cuales no proporcionan un nivel adecuado de protección de datos personales, según lo publicado por la Comisión Europea el 4 de junio de 2021, y su actualización periódica.
   6. En caso de que estas definiciones restrinjan o reduzcan el alcance de las definiciones relacionadas según la Ley de Protección de Datos, la definición se ampliará para que coincida con la definición según esa Ley.
   7. En ausencia de una definición en virtud de esta Sección, un término se interpretará de manera que cumpla con todas las Leyes de Protección de Datos aplicables.
6. *Interpretación*.
   1. Los términos definidos utilizados en este DSA pero no definidos aquí tendrán el significado especificado en otras partes de este Acuerdo.
   2. Las palabras “incluye” e “incluido” se interpretarán en el sentido de “incluir, entre otros”.
   3. Al cumplir con sus obligaciones bajo el Acuerdo de Servicios y este DSA, las Partes reconocen que la política corporativa de MSD y sus Afiliadas exige que los negocios de MSD se realicen dentro de la letra y el espíritu de cualquier Ley de Protección de Datos aplicable, lo que incluye el Reglamento General de Protección de Datos de la UE. En el caso de que ambas Partes no estén sujetas a las mismas Leyes de Protección de Datos, se espera que ambas Partes cumplan con todos los estándares de protección de datos razonablemente relevantes contenidos en dichas leyes.
   4. En relación con el Propósito del intercambio de datos en virtud del Acuerdo, el Proveedor puede Procesar Información personal de una afiliada de la Compañía o más. En tal caso, cualquiera de esas afiliadas de la Compañía se considerará un “Controlador” de la Información personal y un beneficiario externo de este DSA, y tendrá derecho a basarse en todos los derechos y las protecciones otorgados a la Compañía en virtud de este DSA y a hacerlos cumplir, independientemente de si esa afiliada se ha designado como parte del Acuerdo o este DSA.
   5. Este DSA se incorpora y forma parte del Acuerdo.
   6. En caso y en la medida de cualquier conflicto entre los términos del Acuerdo y este DSA, prevalecerán los términos de este DSA, excepto si los términos del Acuerdo protegen más la Información personal Procesada en relación con el Acuerdo, en cuyo caso prevalecerán los términos que brinden más protección de ese Acuerdo.
   7. En caso y en la medida de cualquier conflicto entre los términos de este DSA y las Cláusulas contractuales estándar, prevalecerán los términos de las Cláusulas contractuales estándar.
   8. Excepto que se modifiquen expresamente en este documento, los términos del Acuerdo permanecerán plenamente vigentes.
   9. Si este DSA está redactado en español y en un idioma extranjero, en caso de que haya diferencias entre el texto en español y el texto en el idioma extranjero, prevalecerá el texto en español.
   10. Las secciones y otros títulos de este DSA son solo para facilitar la referencia y no constituirán parte ni afectarán de otro modo el significado o la interpretación de este DSA.
   11. Los anexos y los apéndices de este DSA se considerarán parte integral de este en la misma medida que si se hubieran establecido textualmente en este DSA.
   12. Las disposiciones de este DSA son independientes. Si alguna frase, cláusula o disposición es inválida o inaplicable total o parcialmente, dicha invalidez o inaplicabilidad afectará únicamente a dicha frase, cláusula o disposición, y el resto de este DSA permanecerá plenamente vigente.
   13. Este DSA rige cualquier Procesamiento de Información personal en relación con el Propósito del intercambio de datos y complementa los términos del Acuerdo aplicable al Propósito del intercambio de datos, excepto cuando la Compañía y el Proveedor hayan celebrado otro DSA aplicable a algún Propósito del intercambio de datos.
   14. Este DSA se puede celebrar entre cualquier cantidad de contrapartes, las cuales, en conjunto, constituirán el mismo acuerdo. Cualquier Parte podrá celebrar este DSA mediante la ejecución de dicha contraparte.
   15. Este DSA constituye el acuerdo completo entre las Partes con respecto al asunto de este DSA y (en la medida que lo permita la ley) reemplaza todas las representaciones o los acuerdos orales o escritos anteriores entre las Partes con respecto a ese tema, siempre que nada de lo incluido en este DSA y ninguna de las Partes intenten excluir cualquier responsabilidad por declaraciones fraudulentas.
   16. La ley vigente y las disposiciones de jurisdicción del Acuerdo se aplicarán a este DSA.
7. *Límites de actualizaciones*.
   1. Cuando las Partes renueven, modifiquen, emitan una nueva Declaración de Trabajo bajo, o de cualquier manera modifiquen el Acuerdo o cualquier Declaración de Trabajo bajo el Acuerdo (un "Evento Desencadenante"), el documento más reciente bajo "Data Sharing Addendum (Company Data)" ubicado en <https://www.msdprivacy.com/privacyterms/> reemplazará y sustituirá los términos de este DSA hasta el siguiente Evento Desencadenante, a menos que se presente una objeción dentro de los 30 días siguientes a la ocurrencia del evento desencadenante. No obstante lo anterior, puede haber situaciones que requieran una enmienda inmediata a los términos de este DSA, lo cual solo ocurrirá por razones articuladas en 7(b), y solo se hará de buena fe y después de asegurar que los nuevos términos o términos modificados se limiten a aquellos necesarios para cumplir con la nueva Ley de Protección de Datos aplicable, jurisprudencia o guías emitidas por las autoridades de protección de datos relevantes.
   2. En el evento de que ocurra cualquiera de los siguientes escenarios, las Partes acuerdan de inmediato con los términos más recientes publicados en la dirección anterior, a menos que se presente una objeción dentro de los 30 días tras el aviso de la Compañía de los nuevos términos proporcionados a todas las entidades que han solicitado recibir aviso en [privacy\_updates@msd.com](mailto:privacy_updates@msd.com):  
      1. la Ley de Protección de Datos aplicable ha sido actualizada de manera que los términos contractuales existentes de este DSA son inadecuados para satisfacer los requisitos de la ley actualizada,
      2. hay un cambio en la Ley de Protección de Datos aplicable y las Partes tienen un interés razonable y legítimo en modificar estos términos debido al cambio de ley, por ejemplo y sin limitación, eliminando requisitos que ya no son necesarios, o
      3. hay nueva jurisprudencia o guías emitidas por las autoridades de protección de datos relevantes que tienen un efecto comparable a un cambio en la ley descrito en (i) o (ii) arriba.
8. *Aplicabilidad de los Apéndices*. Las Cláusulas contractuales estándar adjuntas al presente como Apéndice 2 y los anexos adjuntos como Apéndice 3 se aplicarán únicamente en la medida en que lo exija la Ley de Protección de Datos aplicable. Las Partes acuerdan cumplir con dichas cláusulas y anexos únicamente en la medida en que se alineen y sean necesarios en virtud de los requisitos de la Ley de Protección de Datos aplicable en cada jurisdicción respectiva.
9. *Aviso*. Los avisos proporcionados en virtud de este DSA (cada uno un “Aviso”) se realizarán por escrito. Los Avisos proporcionados en virtud de este DSA se realizarán de conformidad con las disposiciones de aviso del Acuerdo aplicable, junto con las copias enviadas a la Compañía por correo electrónico, a [msd\_privacy\_office@msd.com](mailto:msd_privacy_office@msd.com), marcadas con una línea de asunto de “DSA Notice from Supplier” (Aviso de DSA por parte del Proveedor) o, en el caso de un Incumplimiento de datos personales, “Urgent: Personal Data Breach Notice” (Urgente: Aviso de Incumplimiento de datos personales).

**APÉNDICE 1: Medidas de seguridad de Tecnología de la Información**

1. Definiciones – Cuando se utiliza en este Anexo, cada uno de los siguientes términos definidos tendrá la definición que se da a continuación para ese término. Los términos definidos utilizados en este Anexo pero no definidos aquí tendrán el significado especificado en otro lugar del Acuerdo.
   1. “Información de la Compañía” significa cualquier información de la Compañía o de cualquiera de las Afiliadas de la Compañía o de sus respectivos proveedores, clientes u otros socios comerciales proporcionada a, obtenida por, creada o generada por o procesada de otra manera por el Proveedor o cualquiera de los proveedores de servicios de terceros del Proveedor en relación con cualquiera de los Servicios y cualquier otra información que deba ser tratada como confidencial bajo el Acuerdo.
   2. “Violación de Datos” significa una destrucción, pérdida, alteración, uso, transmisión o divulgación accidental o no autorizada de o acceso a cualquier Información de la Compañía.
   3. “Punto Final” significa cualquier computadora, incluyendo cualquier portátil o de escritorio, dispositivo móvil, equipo de laboratorio, servidor u otro dispositivo en los Sistemas del Proveedor, incluyendo cualquier alojado en un sitio de terceros externo (por ejemplo, proveedor de nube).
   4. “Evento de Notificación” significa cualquier evento, incluyendo una Violación de Datos, que requiere la notificación de individuos o entidades bajo cualquier Ley.
   5. “Evento de Seguridad” significa cualquier A) Violación de Datos, (B) Evento de Notificación, (C) acceso no autorizado a o interferencia con las operaciones de los Sistemas del Proveedor o (D) violación de las obligaciones de seguridad del Proveedor bajo este Anexo, el Acuerdo o cualquier Ley.
   6. “Software Sujeto” significa cualquier software proporcionado o utilizado en conexión con cualquiera de los Servicios, incluyendo cualquier software entregado a, o instalado en cualquier computadora, incluyendo cualquier portátil o de escritorio, dispositivo móvil, equipo de laboratorio, servidor, otro dispositivo u otro componente de, o conectado a, los sistemas de información de, la Compañía o cualquiera de las Afiliadas de la Compañía.
   7. “Sistemas del Proveedor” significa las redes del Proveedor y todos los sistemas, incluyendo el Software Sujeto, (A) proporcionado o utilizado en conexión con cualquiera de los Servicios, (B) en los que cualquier Información de la Compañía o entregables o trabajo en progreso para la Compañía o sus Afiliadas, se almacena o se procesa de otra manera o desde los que se accede, (C) conectado a la información, red u otros sistemas de la Compañía o sus Afiliadas o desde los que se puede acceder a la información, red u otros sistemas de la Compañía o sus Afiliadas, o (D) a los que cualquiera de los anteriores puede estar conectado o desde los que cualquiera de los anteriores puede ser accedido.
2. Seguridad de la Red - El Proveedor mantendrá políticas, procedimientos y controles de seguridad de la red y realizará actividades de seguridad de la red, consistentes con las mejores prácticas en la industria del Proveedor, pero que como mínimo incluyen la provisión de firewall de red, controles de detección y prevención de intrusiones, controles de protección contra ataques de denegación de servicio distribuido (DDoS) y evaluaciones de vulnerabilidad y pruebas de penetración realizadas regularmente, de acuerdo con las mejores prácticas en la industria del Proveedor (pero no menos frecuentemente que anualmente). En ningún caso las políticas, procedimientos o controles de seguridad de la red del Proveedor aplicados a la protección de la Información de la Compañía y los Sistemas del Proveedor serán menos rigurosos y protectores que los aplicados por el Proveedor a la protección de su propia información y sus otros sistemas de naturaleza similar.
3. Seguridad de la Aplicación - Basado en la naturaleza de los servicios proporcionados, si corresponde, el Proveedor deberá tener procesos y controles del ciclo de vida del desarrollo de software ("Proceso SDLC") que rigen el desarrollo de y los cambios en cualquier Software del Proveedor, incluyendo actualizaciones, mejoras, parches, mejoras, correcciones de errores, modificaciones, mejoras, correcciones, revisiones, lanzamientos y otros cambios. El Proceso SDLC deberá, como mínimo, incluir prácticas reconocidas y comparables de desarrollo de software seguro de estándares de la industria. El Proveedor deberá seguir un proceso de gestión de parches que asegure que los Sistemas de Información del Proveedor estén actualizados con la seguridad y funcionalidad apropiadas. El Proveedor deberá remediar y volver a probar cualquier vulnerabilidad identificada de manera oportuna, acorde con el riesgo, y dentro de los plazos proporcionados en las Políticas y Procedimientos del Proveedor.
4. Seguridad de Datos - Basado en la naturaleza de los servicios proporcionados, si corresponde, el Proveedor deberá manejar, almacenar y procesar de otra manera la Información de la Compañía, de acuerdo con prácticas y estándares de la industria reconocidos y comparables, como los establecidos en el párrafo 11 (incluyendo PCI DSS, si corresponde) y de acuerdo con todas las Leyes. El Proveedor deberá establecer y mantener salvaguardas razonables contra una Violación de Datos. Además de y sin limitar ninguna otra de las obligaciones del Proveedor, el Proveedor deberá almacenar toda la Información de la Compañía de acuerdo con las mejores prácticas en la industria del Proveedor y en cumplimiento de todas las Leyes, y deberá utilizar medidas de seguridad que cumplan con las mejores prácticas en la industria del Proveedor, incluyendo encriptación y firewalls, para proteger la Información de la Compañía de una Violación de Datos. Cuando el Proveedor almacena la Información de la Compañía en una instalación fuera del sitio, el Proveedor debe haber cumplido con todos los términos en el Acuerdo o en cualquier acuerdo ejecutado en conexión con el Acuerdo, relacionado con la divulgación de la Información de la Compañía a terceros o de otra manera involucrando a terceros para proporcionar o asistir en la provisión de productos o servicios, y el Proveedor deberá utilizar una instalación de almacenamiento fuera del sitio razonablemente aceptable para la Compañía que deberá, sin limitar lo anterior, estar en pleno cumplimiento con todas las disposiciones de este Anexo. Además, el proveedor de dicha instalación de almacenamiento fuera del sitio debe estar vinculado por un acuerdo de confidencialidad escrito entre el Proveedor y dicho proveedor, que contiene términos no menos estrictos que los del Acuerdo o cualquier acuerdo ejecutado en conexión con el Acuerdo y que protege toda la Información de la Compañía almacenada en el mismo.
5. Almacenamiento de Datos - Basado en la naturaleza de los servicios proporcionados, si corresponde, toda y cualquier Información de la Compañía será manejada, almacenada y procesada de otra manera únicamente en los recursos de computación y almacenamiento designados por el Proveedor. La Información de la Compañía sólo será manejada, almacenada o procesada de otra manera en o transferida a un portátil o dispositivo móvil, si (A) es un portátil o dispositivo móvil del Proveedor, (B) el Proveedor encripta toda la Información de la Compañía en ese portátil o dispositivo móvil de acuerdo con los estándares de encriptación en el párrafo 7 a continuación y (C) ese portátil o dispositivo móvil está sujeto a controles de Endpoint consistentes con prácticas y estándares de la industria reconocidos y comparables, como los establecidos en el párrafo 11. La Información de la Compañía no será manejada, almacenada o procesada de otra manera en un dispositivo portátil, excepto como se proporciona en la frase inmediatamente anterior. El Proveedor deberá almacenar todas las copias de seguridad de la Información de la Compañía como parte de sus procesos de respaldo y recuperación designados, y dichas copias de seguridad de la Información de la Compañía deben estar encriptadas de acuerdo con este Anexo, incluyendo los requisitos de este párrafo 5 y el párrafo 7 a continuación.
6. Transmisión de Datos - Basado en la naturaleza de los servicios proporcionados, si corresponde, cualquier transmisión o intercambio electrónico de Información de la Compañía se realizará por medios seguros (utilizando HTTPS o SFTP o equivalente) que sean consistentes con prácticas y estándares de la industria reconocidos y comparables, como los establecidos en el párrafo 11, y únicamente de acuerdo con el párrafo 7 a continuación.
7. Encriptación de Datos - Basado en la naturaleza de los servicios proporcionados, si corresponde, además de y sin limitar ninguna otra obligación del Proveedor, el Proveedor acepta que cualquier Información de la Compañía compuesta por Información Personal sujeta a protección bajo cualquier Ley o compuesta por información sujeta a protección bajo el estándar de Protección de Datos de la Industria de Tarjetas de Pago vigente, incluyendo todos los datos de respaldo de la Compañía, se mantendrá en forma encriptada, utilizando una solución de encriptación comercialmente soportada. El Proveedor acepta que se desplegarán soluciones de encriptación que encripten la Información de la Compañía de acuerdo con prácticas y estándares de la industria reconocidos y comparables, como los establecidos en el párrafo 11, pero con no menos de una clave de 128 bits para encriptación simétrica y una longitud de clave de 2048 (o mayor) bits para encriptación asimétrica.
8. Reutilización de Datos - Basado en la naturaleza de los servicios proporcionados, si corresponde, el Proveedor utilizará toda y cualquier Información de la Compañía únicamente para los propósitos de realizar los Servicios. El Proveedor no distribuirá, reutilizará ni compartirá en otras aplicaciones, entornos o unidades de negocio del Proveedor ninguna Información de la Compañía.
9. Manejo de Datos al Final del Acuerdo - Basado en la naturaleza de los servicios proporcionados, si corresponde, además de y sin limitar ninguna otra obligación del Proveedor, a petición de la Compañía y excepto como se proporciona de otra manera en el Acuerdo, a la expiración o terminación anticipada del Acuerdo, toda la Información de la Compañía en posesión o control del Proveedor o cualquiera de los afiliados, subcontratistas, proveedores de servicios, agentes u otros consultores del Proveedor será destruida o devuelta, según elija la Compañía.
10. Notificación de Brecha de Seguridad - Además de y sin limitar ninguna otra obligación del Proveedor, el Proveedor notificará a la Compañía de un Evento de Seguridad real o razonablemente sospechado dentro de las 24 horas de haberse enterado de dicho Evento de Seguridad real o razonablemente sospechado. El Proveedor notificará a la Compañía de dicho Evento de Seguridad real o razonablemente sospechado contactando al equipo de Seguridad de la Compañía por teléfono (+1-704-345-6700 – Elija la Opción 1) y correo electrónico al Centro de Operaciones Globales [globalopscnt@merck.com](mailto:globalopscnt@merck.com). El Proveedor proporcionará información y asistencia que la Compañía pueda solicitar razonablemente con respecto a un Evento de Seguridad, incluyendo información de causa raíz.
11. Estándares de la Industria - Los estándares de la industria generalmente reconocidos incluyen, pero no se limitan a, los estándares y referencias actuales establecidos y mantenidos por los siguientes:
    1. Centro para la Seguridad de Internet - ver [http://www.cisecurity.org](http://www.cisecurity.org/)
    2. Industria de Tarjetas de Pago / Estándares de Seguridad de Datos (PCI/DSS) – ver <http://www.pcisecuritystandards.org/>
    3. Instituto Nacional de Estándares y Tecnología - ver [http://csrc.nist.gov](http://csrc.nist.gov/)
    4. Ley Federal de Gestión de Seguridad de la Información (FISMA) - ver [http://csrc.nist.gov](http://csrc.nist.gov/)
    5. ISO/IEC serie 27000 - ver <http://www.iso27001security.com/>
    6. Organización para el Avance de los Estándares de Información Estructurada (OASIS) – ver <http://www.oasis-open.org/>
    7. El Proyecto de Seguridad de Aplicaciones Web Abiertas (OWASP) – ver [http://www.owasp.org](http://www.owasp.org/)
    8. La CWE (Enumeración de Debilidades Comunes) - ver [http://cwe.mitre.org](http://cwe.mitre.org/) o CWE/SANS Top 25 Errores de Programación - <http://cwe.mitre.org/top25/>
    9. El Instituto SANS- ver [http://www.sans.org](http://www.sans.org/)
    10. Errores de Software Más Peligrosos <http://www.sans.org/top25-programming-errors/>
    11. A petición razonable de la Compañía, el Proveedor permitirá a la Compañía auditar el cumplimiento del Proveedor con los requisitos enumerados anteriormente. El Proveedor corregirá cualquier incumplimiento de los requisitos, tan pronto como sea razonablemente posible.

**APÉNDICE 2**

En caso de que la Compañía exporte Información personal de una manera que requiera el Módulo 1 de las Cláusulas contractuales estándar, se aplicarán los siguientes términos:

*Se incorpora al presente como referencia el texto del cuerpo del Módulo 1 (Controlador a Controlador) de las Cláusulas contractuales estándar adjuntas a la decisión de implementación (UE) 2021/914 de la Comisión del 4 de junio de 2021. Los aspectos opcionales se describen a continuación:*

1. *Se omite la cláusula 7 (cláusula de atraque).*
2. *Para la cláusula 11, se omite el texto opcional.*
3. *Para la cláusula 17, se elige la opción 1; el estado miembro es Países Bajos.*
4. *Para la cláusula 18, el foro elegido son los Países Bajos.*

**ANEXO I AL APÉNDICE 2**

**A. LISTA DE PARTES**

*Consulte el Acuerdo*

**B. DESCRIPCIÓN DE LA TRANSFERENCIA**

*Consulte el Anexo del Acuerdo titulado “Detalles del Procesamiento de datos”.*

**C. AUTORIDAD DE SUPERVISIÓN COMPETENTE**

****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/)

**ANEXO 2 AL APÉNDICE 2: MEDIDAS TÉCNICAS Y ORGANIZATIVAS**

Consulte el Apéndice 1 del DSA al que se adjuntan estas Cláusulas. Además, el importador de datos se asegurará de que todos los datos personales estén seudonimizados y cifrados cuando corresponda. Además, al recibir una solicitud de una autoridad gubernamental relacionada con los datos personales sujetos a estas Cláusulas, el importador de datos y sus afiliadas garantizan que (i) las demandas de acceso por parte de servicios de inteligencia o autoridades similares en los EE. UU. o en otros lugares, y (ii) cualquier “deber de divulgación” de los datos personales descritos en el Anexo 1B será impugnado por el Importador de datos y sus afiliadas de conformidad con las leyes y las regulaciones aplicables antes de su extracción.

**APÉNDICE 3**

**Requisitos legales estatales, nacionales, regionales y provinciales adicionales**

**ANEXO DEL REINO UNIDO: Ley de Protección de Datos de 2018**

Este Apéndice 3 incorpora como referencia el Anexo de Transferencia internacional de datos a las Cláusulas contractuales estándar de la Comisión de la UE, versión B1.0, vigentes al 21 de marzo de 2022, se considerará ejecutado en su totalidad por todas las partes del Acuerdo, cubrirá todas las transferencias aplicables según el DSA e incluirá todas las cláusulas obligatorias de la Parte 2.

**ANEXO DE SUIZA: FADP**

1. En la medida en que las transferencias de datos descritas en el Apéndice 2 estén sujetas a la Ley Federal sobre Protección de Datos (Federal Act on Data Protection, “FADP”), las referencias al Reglamento General de Protección de Datos (General Data Protection Regulation, RGPD) deben entenderse como referencias a la Ley Federal sobre Protección de Datos de Suiza.
2. Durante el tiempo que lo exija la FADP, los datos personales de las personas jurídicas estarán protegidos de conformidad con estas Cláusulas al igual que las personas físicas que sean sujetos de datos.
3. Cláusula 13: Supervisión paralela
   1. Cuando la transferencia de datos se rige por la FADP: El Comisionado Federal de Protección de Datos e Información (Federal Data Protection and Information Commissioner, “FDPIC”) es el organismo de supervisión competente.
   2. Cuando la transferencia de datos se rige por el GDPR: Se aplicarán los criterios de la Cláusula 13(a).
4. Cláusula 18(c): Elección de foro y jurisdicción: un sujeto de datos que tenga su residencia habitual en Suiza también podrá presentar acciones judiciales contra el exportador o el importador de datos ante los tribunales de Suiza.

**ANEXO DE CANADÁ: Ley 25 de Quebec**

* + - 1. Cualquier aviso requerido en virtud de este DSA en relación con un Incumplimiento de datos personales, y cualquier aviso similar requerido en virtud del Acuerdo, también será necesario para eventos que constituyan un incumplimiento o intento de incumplimiento de este DSA por parte del Proveedor.
      2. Si se requiere obtener consentimiento en relación con los términos de este DSA, el Proveedor también debe conservar la evidencia de todos los consentimientos durante tres (3) años después de la finalización del Acuerdo.

**ADENDA DE EMIRATOS ÁRABES UNIDOS: Ley Federal No. 45 de 2021 sobre la Protección de Datos Personales**

1. En la medida en que las transferencias de datos descritas en el Apéndice 2 estén sujetas a la Ley Federal No. 45 de 2021 de los Emiratos Árabes Unidos sobre la Protección de Datos Personales ("PDPL"), a menos que y hasta que la Oficina de Datos de los EAU emita sus propias cláusulas contractuales estándar para legitimar la transferencia de Información Personal fuera de los Emiratos Árabes Unidos y las Partes hayan celebrado dichas cláusulas contractuales estándar, las Partes acuerdan que las Cláusulas Contractuales Estándar adjuntas en el Apéndice 2 se aplicarán, mutatis mutandis, en relación con dichas transferencias para proporcionar garantías adecuadas para la Información Personal y los Sujetos de Datos. A estos efectos: a. Las referencias a "Reglamento (UE) 2016/679", "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y sobre la libre circulación de estos datos (Reglamento General de Protección de Datos)" y "dicho Reglamento" se reemplazan por "PDPL". b. Las referencias a artículos específicos del "Reglamento (UE) 2016/679" se reemplazan con el artículo o sección equivalente del PDPL. c. Las referencias a la "Unión Europea", "Unión", "UE", "Estado Miembro de la UE", "Estado Miembro" y "UE o Estado Miembro" se reemplazan con "Emiratos Árabes Unidos". d. La "autoridad de supervisión competente" y la "autoridad de supervisión" se reemplazan con la "Oficina de Datos". e. Cualquier disputa que surja de las Cláusulas Contractuales Estándar se regirá por las leyes de los Emiratos Árabes Unidos y se resolverá por los tribunales de los Emiratos Árabes Unidos. Las Partes acuerdan someterse a la jurisdicción de dichos tribunales. f. Si existe alguna incoherencia o conflicto entre el PDPL y las Cláusulas Contractuales Estándar adjuntas en el Apéndice 2, se aplicará el PDPL. g. Si el significado de las Cláusulas Contractuales Estándar adjuntas en el Apéndice 2 no es claro en la medida en que se apliquen a transferencias de Información Personal fuera de los EAU, o si existe más de un significado, se aplicará el significado que más se alinee con el PDPL.
2. Si la Oficina de Datos de los EAU emite sus propias cláusulas contractuales estándar para legitimar la transferencia de Información Personal fuera de los Emiratos Árabes Unidos, las Partes negociarán de buena fe con miras a acordar e implementar las cláusulas contractuales estándar tan pronto como sea razonablemente posible. Cuando las Partes celebren cláusulas contractuales estándar de acuerdo con la oración anterior, dichas cláusulas contractuales estándar reemplazarán, en relación con las transferencias de Información Personal sujetas al PDPL fuera de los Emiratos Árabes Unidos, a las Cláusulas Contractuales Estándar adjuntas en el Apéndice 2 como las garantías adecuadas implementadas para proporcionar garantías adecuadas para la Información Personal y los Sujetos de Datos en relación con las transferencias.
3. La Compañía podrá revocar su acuerdo de estar vinculada por las Cláusulas Contractuales Estándar adjuntas en el Apéndice 2 mediante notificación por escrito al Proveedor cuando la Oficina de Datos adopte una decisión de adecuación que cubra la transferencia de Información Personal a la que se aplican las Cláusulas Contractuales Estándar, o la Compañía determine de otra manera que se aplican otras garantías adecuadas en relación con la transferencia. A partir de la fecha de cualquier notificación emitida por la Compañía de acuerdo con la oración anterior, las Cláusulas Contractuales Estándar adjuntas en el Apéndice 2 dejarán de aplicarse a las transferencias de Información Personal sujetas al PDPL fuera de los Emiratos Árabes Unidos.

**ADENDA DE BRASIL: LGPD - Cláusulas Contractuales Estándar**

Las Cláusulas Contractuales Estándar de Brasil ("SCCs") bajo la Ley General de Protección de Datos (Lei Geral de Proteção de Dados – “LGPD”) deben ser observadas cuando se procesen datos de residentes brasileños o cuando cualquier transferencia de datos requiera su aplicación. Las partes acuerdan adoptar las SCCs en su totalidad, tal como las emite la Autoridad Nacional de Protección de Datos de Brasil (“ANPD”), salvo que se modifiquen de acuerdo con los términos permitidos expresamente por las cláusulas. Dichas SCCs se incorporan al Acuerdo por referencia, con las siguientes selecciones hechas donde se presentan varias opciones de texto:

OPCIÓN B se selecciona para la Sección 3.1. El Importador podrá realizar una Transferencia Posterior de Datos Personales sujeta a la Transferencia Internacional de Datos regulada por estas Cláusulas, en los casos y condiciones descritas a continuación y las disposiciones de la CLÁUSULA 18.

OPCIÓN A se selecciona para la Sección 4.1. Sin perjuicio del deber de asistencia mutua y las obligaciones generales de las Partes, la Parte Designada a continuación será principalmente responsable de cumplir con las siguientes obligaciones establecidas en estas Cláusulas:

a) Responsable de publicar el documento proporcionado en la CLÁUSULA 14:

[x] Exportador [ ] Importador

b) Responsable de responder a las solicitudes de los Titulares de los Datos tratadas en la CLÁUSULA 15:

[x] Exportador [ ] Importador

c) Responsable de notificar el incidente de seguridad previsto en la CLÁUSULA 16:

[x] Exportador [ ] Importador

**ADENDA DE ARABIA SAUDITA: PDPL - Cláusulas Contractuales Estándar**

Las Cláusulas Contractuales Estándar de Arabia Saudita ("SCCs") bajo la Ley de Protección de Datos Personales ("PDPL") se incorporarán cuando se procesen datos de residentes saudíes, cuando una transferencia de datos esté sujeta a la jurisdicción saudí o cuando la ley saudí exija cumplir con las SCCs de Arabia Saudita. La versión de las SCCs alineada con el tipo de plantilla descrita en el Anexo 2 es aplicable en su totalidad y se incorpora al Acuerdo por referencia.